COUNCIL OF THE EUROPEAN UNION

Brussels, 30 June 2014 (OR. en)

11109/14

Interinstitutional File: 2012/0010 (COD)

LIMITE

DATAPROTECT 95
JAI 541
DAPIX 90
FREMP 128
COMIX 327
CODEC 1504

NOTE

From:	Presidency
To:	Delegations
Subject:	Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

Delegations find attached a revised version of the draft proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. This version seeks to take account of the discussions on the draft Directive that took place in the Working Party on Information Exchange and Data Protection under the Greek Presidency.

All changes made to the original Commission proposal are underlined text, or, where text has been deleted, indicated by (…). Where existing text has been moved, this text is indicated in italics. The most recent changes are marked in bold underlining.

ANNEX

2012/0010 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data[1]

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national Parliaments,

After consulting the European Data Protection Supervisor[2],

Acting in accordance with the ordinary legislative procedure,

---

1 ES, HU, IT, LV, PT, SI, UK scrutiny reservation on the whole text. FI scrutiny reservation since FI meant that the GDPR should be dealt with first.

2 OJ C… , p.

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is **a** fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty of the Functioning of the European Union lay down that everyone has the right to the protection of personal data concerning him or her.

(2) The (…) principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice.

(3) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data collection and sharing has increased spectacularly. Technology allows (…) to make use of personal data on an unprecedented scale in order to pursue (…) activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(4) This requires facilitating the free flow of data between competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences, and for these purposes, safeguarding public security or the execution of criminal penalties within the Union and the transfer to third countries and international organisations, while ensuring a high level of protection of personal data. These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement.

(5) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[3] applies to all personal data processing activities in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Community law', such as activities in the areas of judicial co-operation in criminal matters and police co-operation.

[3] OJ L 281, 23.11.1995, p. 31.

(6) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters[4] applies in the areas of judicial co-operation in criminal matters and police co-operation. The scope of application of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States.

(7) Ensuring a consistent and high level of protection of the personal data of individuals and facilitating the exchange of personal data between competent public authorities of Members States is crucial in order to ensure effective judicial co-operation in criminal matters and police cooperation. To that aim, the level of protection of the rights and freedoms of individuals with regard to the processing of personal data by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences and for these purposes**, (…)** safeguarding public security or the execution of criminal penalties should be equivalent in all Member States. Effective protection of personal data throughout the Union requires strengthening the rights of data subjects and the obligations of those who process personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States. [5]

(8) Article 16(2) of the Treaty on the Functioning of the European Union mandates the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.

(9) On that basis, Regulation EU …../2012 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) lays down general rules to protect of individuals in relation to the processing of personal data and to ensure the free movement of personal data within the Union.

---

4 OJ L 350, 30.12.2008, p. 60.

5 UK suggested the deletion of this recital since the case has not been made for the need of equivalent standards of data protection in all MS and is not in line with the subsidiarity principle.

(10) In Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal matters and police co-operation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the Conference acknowledged that specific rules on the protection of personal data and the free movement of such data in the fields of judicial co-operation in criminal matters and police co-operation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.

(11) Therefore a distinct Directive should meet the specific nature of these fields and lay down the rules relating to the protection of individuals with regard to the processing of personal data by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences and for these purposes, (…) safeguarding public security, or the execution of criminal penalties.[6] **Such competent public authorities may also include bodies/entities entrusted by national law to perform, as their predominant task, public duties or exercise public powers for the purposes of prevention, investigation, detection or prosecution of criminal offences and for these purposes, safeguarding public security, or the execution of criminal penalties. However where such body/entity processes personal data for other purposes than for the performance of public duties and/or the exercise of public powers for the prevention, investigation, detection or prosecution of criminal offences, and for these purposes safeguarding public security, or the execution of criminal penalties, Regulation XXX applies. Therefore Regulation XXX applies in cases where a public or private entity, collects personal data for other purposes and processes those personal data further for compliance with a legal obligation to which it is subject *e.g.* where providers of publicly available electronic communications services or of public communications network retain for the purpose of investigation, detection and prosecutions of serious crime certain data which are generated or processed by them, and provide those data only to the competent national authorities in specific cases and in accordance with national law. A public or private entity, which processes personal data on behalf of such authorities or bodies/entities within the scope of this Directive should be bound, by a contract or other legal act and the provisions applicable to processors pursuant to this Directive, while the application of Regulation XXX remains unaffected for processing activities of the processor outside the scope of this Directive.**[7]

---

6 CH wanted to add the following sentence in the end of the recital: "At the same time the legitimate activities of the competent public authorities should not be jeopardized in any way."

7 FI scrutiny reservation and SE reservation. ES found that the recital neither defined nor clarified what was meant with *bodies/entities.* SE meant that the scope of the Directive should be set out in the body of the text. SE found the text in particular the last sentence very prescriptive.

(12) In order to ensure the same level of protection for individuals through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent public authorities, the Directive should provide harmonised rules for the protection and the free movement of personal data (…) processed for the purposes of prevention, investigation, detection or prosecution of criminal offences and for these purposes safeguarding public security or the executions of criminal penalties. The approximation of Member States' laws should not result in any lessening of the data protection they afford but should, on the contrary, seek to ensure a high level of protection within the Union. Member States should not be precluded from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent public authorities.[8]

(13) This Directive allows the principle of public access to official documents to be taken into account when applying the provisions set out in this Directive.

(14) The protection afforded by this Directive should concern natural persons, whatever their nationality or place of residence, in relation to the processing of personal data.

(15) The protection of individuals should be technologically neutral and not depend on the technologies, mechanisms or procedures used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means, as well as to manual processing if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Directive. This Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, such as an activity[9] concerning national security, taking into account Articles 3 and 6 of the Treaty on the Functioning of the European Union, nor [10] to data processed by the Union institutions, bodies, offices and agencies, such as Europol or Eurojust. [11]

---

[8] RO meant that recital 12 would entail multiple negative consequences for the implementation and wanted police work and domestic processing out of the scope of the Directive. FI scrutiny reservation

[9] FR suggested to change "activity" into "such as *activities* …"

[10] FR suggested to add the following text: "nor does it cover the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union". BE asked what would happen with data generated from national security and the police sector, under what regime they would fall. UK meant that the part on national security should be inserted into the body of the text.

[11] AT did not find recital 15 clear.

(15a) Regulation (EC) No 45/2001[12] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal instruments applicable to such processing of personal data should be adapted to the principles and rules of Regulation EU …../2012.

15b While this Directive applies also to the activities of courts and other judicial authorities[13], it does not preclude Member States from specifying processing operations and processing procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular as regards personal data contained in a judicial decision or in records during criminal proceedings. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. [14]

(16) The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous information, that is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is no longer identifiable. **[15]** [16]

---

12 OJ L 8, 12.1.2001, p. 1.

13 CH found it necessary to define activities of courts and other judicial authorities.

14 BE reservation of substance and SE scrutiny reservation. IE welcomed recital 15b and wanted the text, in particular the part relating to the independence of the judges to be put into the body of the text. Cion also welcomed the recital on courts.

15 Cion welcomed the redrafting of recital 16 ensuring consistency between GDPR and the Directive.

16 CH suggested to insert a recital with the following text: "The transmitting Member State should have the possibility to subject the processing by the receiving Member State to conditions in particular with regard to the purpose for which personal data could be used, but it should not refuse the transmission of information to this State on the simple grounds that this State does not have an adequate data protection level." CH added the underlined sentence.

(16a) Genetic data should be defined as personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained.[17]

(17) Personal data relating to health should include in particular (…) data pertaining to the health status of a data subject, (…) including any information on, for example, a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as for example from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

(18) Any processing of personal data must be (…)lawful and fair in relation to the individuals concerned, for specific purposes laid down by law.[18]

(19) For the prevention, investigation and prosecution of criminal offences and for these purposes, (…)[19]safeguarding public security, it is necessary for competent public authorities to (…) process personal data, collected in the context of the prevention, investigation, detection or prosecution of specific[20] criminal offences beyond that context to develop an understanding of criminal phenomena and trends, to gather intelligence about organised criminal networks, and to make links between different offences detected.

---

17 SE expressed concerns with recital 16a because of DNA profiles with the purpose of identifying should not be allowed to be used in the future.

18 ES suggested to delete the second sentence since data can be collected for numerous reasons and serve a number of purposes. FR preferred the previous drafting of recital 18.

19 BE wanted to add the following text: "and the prevention of danger".

20 ES wanted to delete "specific" since crime prevention was not about a specific crime but related to group of offences or all offences.

19a In order to maintain security of the processing and to prevent processing in breach of this Directive, personal data should be processed in a manner that ensures an appropriate level of security and confidentiality, taking into account available state of the art and technology and the costs of implementation in relation to the risks and the nature of the personal data to be protected.

(20) Personal data should not be processed for purposes incompatible with the purpose for which it was collected. In general, further processing for historical, statistical or scientific purposes should not be considered as incompatible with the original purpose of processing. Personal data should be adequate, relevant and not excessive for the purposes for which the personal data are processed. (…). Personal data which are inaccurate should be rectified or erased. [21]

(21) The principle of accuracy of data should be applied taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of individuals and are in some cases not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

(22) In the interpretation and application of the provisions of this Directive, by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences and for these purposes, safeguarding public security, or the execution of criminal penalties, account should be taken of the specificities of the sector, including the specific objectives pursued.

[21] ES suggested removing the last sentence of recital 20. ES meant that requiring that inaccurate data be rectified or erased would make police work ineffective and inefficient since police work consist in receiving and analysing false or incomplete data.

(23) It is characteristic to the processing of personal data (…) by competent public authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences and for these purposes, safeguarding public security or the execution of criminal penalties that personal data relating to different categories of data subjects are processed. Therefore, the competent public authorities (…) should, as far as possible, make a distinction between personal data of different categories of data subjects such as persons convicted of a criminal offence, suspects, (…) victims and third parties. (…).[22]

(24) Furthermore, (…) the competent public authorities should (...) ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. In particular, personal data should be distinguished, as far as possible, according to the degree of their accuracy and reliability; (…) facts should be distinguished from personal assessments in order to ensure both the protection of individuals and the quality and reliability of the information processed by the competent public authorities. [23]

(25) In order to be lawful, the processing of personal data should be necessary for (…) the performance of a task carried out in the public interest by a competent public authority based on Union law or Member State law for the purposes of prevention, investigation, detection or prosecution of criminal offence, and, for these purposes, safeguarding public security, or the execution of criminal penalties. Processing by a competent public authority should also be lawful, where the processing is necessary or in order to protect the vital interests of the data subject or of another person, or for the prevention of an immediate[24] and serious threat to public security.[25]. The data subject's consent should not provide a legal ground for processing personal data by competent public authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the data subject's reaction could not be considered as a freely-given indication of his or her wishes. This should not preclude Member States to provide by law, for example, that an individual could be required for example to agree to the monitoring of his/her location as a condition for probation.

---

22 ES, DK and SE suggested deleting recital 23 since Article 5 was deleted.

23 UK suggested to delete Article 6 as well as recital 24.

24 ES suggested to replace "immediate" because this word is often misinterpreted and replace it with "direct".

25 CH suggested adding the following text after "public security": "Furthermore, a processing of personal data should be lawful if the data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes. **The data subject's consent means any freely-given specific, informed and explicit indication of his or her wishes by which the data subject signifies his agreement to personal data relating to him being processed."** CH considered that excluding *consent* as a legal basis for processing would be an excessive formalism.

(25a) Member States should provide that where[26] Union law or the national law applicable to the transmitting competent public authority provides for[27] specific conditions applicable in specific circumstances to the processing of personal data, [28]the transmitting public[29] authority should inform the recipient to whom data are transmitted about such conditions and the requirement to respect them. Such conditions may for example include that the recipient to whom the data are transmitted does not inform the data subject in case of a limitation to the right of information without the prior approval of the transmitting authority. These obligations apply also to transfers to recipients in third countries or international organisations. Member States should provide that the transmitting public authority does not apply conditions pursuant to paragraph 1[30] to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters IV and V of Title V of the Treaty on the Functioning of the European Union other than those applicable to the transmitting public authority.[31]

[26] BE wanted to replace *where* with *when* (as in Article 7.3 suggested by BE).

[27] BE suggested to delete *for.*

[28] BE suggested to add the following text: these conditions are set out in accordance with the Europol handling codes. The Transmitting ...” (as in Article 7.3 suggested by BE).

[29] BE suggested to delete *public.*

[30] CH wanted to replace "paragraph 1" with "the first sentence".

[31] CH meant that it was necessary to replace "transmitting public authority" at the end of recital 25a with the following: "similar national data transmission" so that Schengen States would be regulated by the same conditions as those applicable to similar national data transmissions. In case where the national law provides for restrictions, those must apply to the national recipient and to the Schengen recipient in the same way.

(26) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights (…) and freedoms, including genetic data, deserve specific protection. This should also include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Directive does not imply an acceptance by the European Union of theories which attempt to determine the existence of separate human races. Such data should not be processed, unless processing is specifically[32] authorised by a law which provides for (…) appropriate safeguards for the rights and freedoms of the data subjects; or if not already authorised by such a law the processing is necessary to protect the vital interests of the data subject or of another person; or the processing is necessary for the prevention of an immediate[33] and serious threat to public security (…). Appropriate safeguards for the rights and freedoms of the data subject may for example include stricter rules on the access of staff of the competent public authority to the data, or the prohibition of transmission of those data. However, the data subject's consent should not provide a legal ground for processing such sensitive personal data by competent public authorities.

(27) Every data subject should have the right not to be subject to a decision which is based solely on profiling (…), unless authorised by law and subject to appropriate safeguards for the rights and freedoms of the data subject (…).

(28) In order to exercise their rights, any information to the data subject should be easily accessible, including on the website of the controller and easy to understand, requiring the use of clear and plain language.

(29) Modalities should be provided for facilitating the data subject's exercise of their rights under the provisions adopted pursuant to this Directive, including mechanisms to request, free of charge, (…) access to data, as well as rectification, erasure and restriction. The controller should be obliged to respond to requests of the data subject without undue delay.

---

32 ES did not see the need to "specifically" to refer to authorisation by law and therefore suggested to delete it.

33 ES suggested to replace "immediate" because this word is often misinterpreted and replace it with "direct".

(30) (…) The data subjects should be informed of at least (…) the identity of the controller, the existence of the processing operation and its purposes, (…) and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, if they do not provide such data.[34]
[35]

(31) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not obtained from the data subject (…), within a reasonable period after obtaining the data, having regard to the specific circumstances in which the data are processed or if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed. [36]

(32) A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals in order to be aware of and verify the lawfulness of the processing. Every data subject should therefore have the right to know about and obtain communication in particular of the purposes for which the data are processed, (…) for what period, and which recipients receive the data, including in third countries. (…)[37]

(33) Member States should be allowed to adopt legislative measures delaying, restricting or omitting the information of data subjects or the access to their personal data to the extent that and as long as such (…) a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties, to protect public security or national security, or, to protect the data subject or the rights and freedoms of others. [38]

---

[34] BE wanted to delete the last sentence because of the burden and cost of this obligation and its suggested suppression of Article 11.1 (aa).

[35] BE suggested a new recital 30a to explain its suggested Article 11.1 "All appropriate measures may include in particular general information on the website of the competent authority."

[36] ES thought that it would more sense to set out the principle as an option rather than an obligation and should be retained only if the principle in recital 33 was also retained.

[37] ES thought that the principle should be fine-tuned and should not jeopardise completed and on-going operations and investigations. ES further thought that the principle could be retained as long as the principle in recital 33 was retained.

[38] ES said that the principle in recital 33 should be the rule and not an exception.

(34) Any refusal or restriction of access should in principle be set out in writing to the data subject including the factual or legal reasons on which the decision is based.

(35) Where Member States have adopted legislative measures restricting wholly or partly the right to access, the data subject should have the right to request that the (…) national supervisory authority checks the lawfulness of the processing. The data subject should be informed of this right. When access is exercised by the supervisory authority on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications by the supervisory authority have taken place and of the result as regards to the lawfulness of the processing in question.

(36) A natural person should have the right to have inaccurate personal data concerning him or her rectified, in particular when pertaining to facts, and the right of erasure where the processing of such data is not in compliance with the provisions laid down in this Directive. However, the right to rectification should not affect, for example, the content of a witness testimony. Where the personal data are processed in the course of a criminal investigation and proceedings, (…) the exercise of the rights of information, access, rectification, erasure and restriction of processing may be carried out in accordance with national rules on judicial proceedings.

(37) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate measures and be able to demonstrate (…) the compliance of processing activities with the rules adopted pursuant to this Directive.[39]

[40]

[39] FR pointed out that specific recitals have been added to the GDPR (recital 60) in order to better define the concept of risk and meant that it could also be useful to include these in this Directive: such as implementing technical and organisation measures for ensuring an appropriate level of security for data protection. These measures should take into account the nature, scope, context and purposes of the processing and the risks for the rights and freedoms of data subjects. Such risks, of varying likelihood or severity, are presented by data processing which could lead to physical, material or moral damage, in particular:

- *where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy, or any other significant economic or social disadvantage; or*
- where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data;
- where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures;
- where personal aspects are evaluated, in particular analysing and prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
- where personal data of vulnerable individuals, in particular of children, are processed;
- where processing involves a large amount of personal data and affects a large number of data subjects.

[40] FR further suggested adding the following two recitals, also taken from the GDPR (recital 60b):
"37a Where personal data are processed on behalf of the controller, the implementation of such measures should include in particular use only of a processor providing sufficient guarantees to implement appropriate technical and organisational measures."
"37b Measures designed to mitigate risks implemented by the controller [or processor] should in particular concern the identification of risks and their assessment in terms of their origin, nature, likelihood and severity."

(38) The protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organisational measures be taken to ensure that the requirements of the Directive are met. In order to be able to demonstrate compliance with the provisions adopted pursuant to this Directive, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. The data protection policies by the controller should specify the application of the data protection rules adopted pursuant to this Directive.[41]

(39) The protection of the rights and freedoms of data subjects as well as the and liability of controllers and processors requires a clear attribution of the responsibilities under this Directive, including where a controller determines the purposes (…) and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller. The carrying out of processing by a processor should be governed by a legal act including a contract[42] binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller.[43]

(40) Processing activities should be recorded by the controller or processor, in order to monitor compliance with this Directive. Each controller and processor should be obliged to co-operate with the supervisory authority and make these records, on request, available to it, so that it might serve for monitoring processing operations.

(41) In order to ensure effective protection of the rights and freedoms of data subjects (…) the controller or processor should consult with the supervisory authority in certain cases prior to intended processing. [44]

---

[41] DE wanted to delete the last part of recital 38 as well as the text in Article 18.1a. Cion said that policies meant guidelines binding for the controller.

[42] SE wanted to delete *including a contract.*

[43] SE found the new text too detailed and questioned it being technically neutral. EE supported recital 39.

[44] NL wanted to see the text of Article 26.2(b) mirrored in the recital.

(42) A personal data breach may, if not addressed in an adequate and timely manner, result in severe material or moral harm (…) to the individual concerned. Therefore, as soon as the controller becomes aware that (…) a personal data breach has occurred which may result in severe material or moral harm, the controller should notify the breach to the supervisory authority without undue delay. The individuals whose personal data (…) could be severely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions (…). [45]

(43) The communication of a personal data breach to the data subject should not be required if the controller has implemented appropriate technological protection measures, and that those measures were applied to the data affected by the personal data breach. Such technological protection measures should include those that render the data unintelligible to any person who is not authorised to access it. Likewise, the communication to the data subject is not required if the controller has taken subsequent measures which ensure that rights and freedoms of affected data subjects are no longer likely to be severely affected (…).

[45] FR suggested to modify recital 42 to read as follows: "(42) A personal data breach may, if not addressed in an adequate and timely manner, result in severe material or moral harm to individuals such as loss of control over their personal data or the limitation of their rights, discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage to the individual concerned. Therefore, as soon as the controller becomes aware that (…). a personal data breach has occurred which may result in severe material or moral harm the controller should notify the breach to the supervisory authority without undue delay. The individuals whose personal data could be severely affected by the breach and who have a right of information over the processing of their personal data should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as severely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it. For example (…) to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay."

(44) (…) A person with expert knowledge of data protection law and practices may assist the controller or processor to monitor internal compliance with the provisions adopted pursuant to this Directive. A data protection officer may be appointed jointly by several public authorities or bodies, taking into account of their organisational structure and size (…). Such data protection officers must be in a position to perform their duties and tasks in an independent (…) manner.[46]

(45) Member States should ensure that a transfer to a third country only takes place if it is necessary for the prevention, investigation, detection or prosecution of criminal offences **, and, for these purposes, safeguarding public security,** or the execution of criminal penalties, and the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level or protection, or when appropriate safeguards have been adduced. [47]

(46) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a **specified** sector**s** within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any specific authorisation.

(47) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should take into account how a given third country respects the rule of law, access to justice, as well as international human rights norms and standards and its general and sectorial law, including legislation concerning public security, defence and national security as well as public order and criminal law.

---

46 CH suggested deleting the last sentence of recital 44.

47 Since DE suggested to remove Article 33.1(c) it suggested to revise recital 45. DE wanted to remove the text restricting transfer only to public authorities because DE meant that it must be possible to make enquiries to companies for example.

(48) The Commission should equally be able to recognise that a third country, or a territory or a **specified** sector within a third country, or an international organisation, no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited except when they are based on an international agreement, appropriate safeguards or a derogation. Provision should be made for procedures for consultations between the Commission and such third countries or international organisations. However, such a Commission decision shall be without prejudice to the possibility to undertake transfers on the basis of appropriate safeguards or on the basis of a derogation laid down in the Directive.

(49) Transfers not based on such an adequacy decision should only be allowed where appropriate safeguards have been adduced in a legally binding instrument, which ensure the protection of the personal data or where the controller (…) has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and, based on this assessment, considers that appropriate safeguards with respect to the protection of personal data exist. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress.
By way of derogation, in specific situations where no adequacy decision or appropriate safeguards exist, a transfer **or a category of transfers** could take place if necessary in order to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides, or where it is essential for the prevention of an immediate[48] and serious threat to the public security of a Member State or a third country, or in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or in individual cases for the establishment, exercise or defence of legal claims.

[48] ES suggested to replace "immediate" because this word is often misinterpreted and replace it with "direct".

(49a) Where personal data are transferred from a Member State to third countries or international bodies, such transfer should, in principle, take place only after the Member State from which the data were obtained has given its authorisation to the transfer. The interests of efficient law enforcement cooperation require that where the nature of a threat to the public security of a Member State or a third country or to the essential interests of a Members State is so immediate as to render it impossible to obtain prior authorisation in good time, the competent public authority should be able to transfer the relevant personal data to the third country concerned without such prior authorisation. [49]

(…)

(51) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions adopted pursuant to this Directive and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data. For that purpose, the supervisory authorities should co-operate with each other and the Commission.

(52) Member States may entrust a supervisory authority already established (…) under Regulation (EU)…./2012 with the responsibility for the tasks to be performed by the national supervisory authorities to be established under this Directive.

[49] DE wanted that it was set out that "prior authorisation" could mean already given authorisation within the EU or generally. CH suggested adding the following sentence in the end of recital 49a: "Furthermore, a transfer of personal data should be lawful if the data subject has given his or her consent to the transfer of his or her personal data for one or more specific purposes." CH considered that processing of personal data should also be lawful if the data subject has given his or her consent to the transfer of his or her personal data. FR wanted to stress that it was for MS to assess all factors that could constitute appropriate and the need to balance all the factors involved.

(53) Member States should be allowed to establish more than one supervisory authority to reflect their constitutional, organisational and administrative structure. Each supervisory authority should be provided with (…) financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and co-operation with other supervisory authorities throughout the Union.

(54) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government or the head of state of the Member State (…).

(55) While this Directive applies also to the activities of national courts and other judicial authorities, the competence of the supervisory authorities should not cover the processing of personal data when they are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks[50]. However, this exemption should be limited to (…) judicial activities in court cases and not apply to other activities where judges might be involved in accordance with national law.

(56) In order to ensure consistent monitoring and enforcement of this Directive throughout the Union, the supervisory authorities should have the same **tasks** and effective powers in each Member State, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings. The investigative powers should include powers of access to data forming the subject matter of processing operations, access to any premises, including to any data processing equipment and means, and powers to collect all the information necessary for the performance of its supervisory **tasks** . These powers should be exercised in conformity with Union law or Member State law. The powers of intervention should include the delivering of opinions before processing is carried out, and ensuring appropriate publication of such opinions, ordering the restriction, erasure or destruction of data, imposing a temporary or definitive ban on processing, warning or admonishing the controller, or drawing a matter to the attention of national parliaments or other political institutions.

50 Several delegations (PL, SI and FI) stressed the importance of this exemption. CH suggested replacing "in order to safeguard …judicial tasks" with the following: "so that it doesn't interfere with national rules on judicial proceedings."

(57) Each supervisory authority should deal with complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.

(58) The supervisory authorities should assist one another in performing their **tasks** and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive.

(59) The European Data Protection Board established by Regulation (EU)…./2012 should contribute to the consistent application of this Directive throughout the Union, including advising the Commission and promoting the co-operation of the supervisory authorities throughout the Union.

(60) Every data subject should, without prejudice to any other administrative or non-judicial remedy, have the right to lodge a complaint with a supervisory authority (…) and have the right to a judicial remedy [51]if they consider that their rights under provisions adopted pursuant to this Directive are infringed or where the supervisory authority does not act on a complaint or does not act where such action is necessary to protect the rights of the data subject.

(61) Any body, organisation or association which aims to protect the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a complaint or exercise the right to a judicial remedy on behalf of a data subject if duly mandated by him or her (…).

[51] CZ wanted to insert the following text after *remedy* "under conditions stipulated by the law of the Member State" to make it possible for the MS to stipulate in national law that the data subject must first exhaust all available administrative remedies before addressing the courts against inaction.

(62) Each natural or legal person should have [52]the right to a judicial remedy against decisions of a supervisory authority concerning them.(…).

(…)

(64) Any damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where they establish fault on the part of the data subject or in case of force majeure.

(65) Penalties should be imposed on any natural or legal person, whether governed by private or public law, that fails to comply with this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and must take all measures to implement the penalties.[53]

(…)

(67) In order to ensure uniform conditions for the implementation of this Directive as regards (…) the adequate level of protection afforded by a third country or a territory or a **specified** sector within that third country or an international organisation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers[54].

---

[52] CZ wanted to add the following text after *have*: "under conditions stipulated by the law of the Member State and to add the following sentence after the first sentence: "Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established. "The addition of the second sentence was to avoid forum shopping.

[53] ES meant that as long as the issue of penalties against public institutions or bodies was not resolved in the GDPR this text should remain in brackets.

[54] OJ L 55, 28.2.2011, p. 13.

(68) The examination procedure should be used for the adoption of measures as regards (…) the adequate level of protection afforded by a third country or a territory or a **specified** sector within that third country or an international organisation, given that those acts are of general scope.[55]

(69) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a **specified** sector within that third country or an international organisation which no longer ensure an adequate level of protection, imperative grounds of urgency so require.

(70) Since the objectives of this Directive, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free exchange of personal data by competent public authorities within the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(71) Framework Decision 2008/977/JHA should be repealed by this Directive.

(72) Specific provisions with regard to the processing of personal data by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in acts of the Union which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, should remain unaffected. The Commission should evaluate the situation with regard to the relationship between this Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, in order to assess the need for alignment of these specific provisions with this Directive.

[55] AT suggested to clarify that that the EDPB is entitled to give an opinion when the Commission adopts adequacy decisions pursuant to Article 34.

(73) In order to ensure a comprehensive and coherent protection of personal data in the Union, international agreements concluded by Member States prior to the entry force of this Directive (…), and which are in compliance with the relevant and applicable Union law prior to the entry into force of this Directive, should remain in force until amended, replaced or revoked. To the extend that such agreements are not compatible with Union law, Member States are[56] required to take all appropriate steps to eliminate any incompatibilities (…).

(74) This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011.[57]

(75) In accordance with Article 6a of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, the United Kingdom and Ireland **are** not bound by the rules laid down in this Directive **which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the Treaty on the Functioning of the European Union** where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial co-operation in criminal matters or police co-operation which require compliance with the provisions laid down on the basis of Article 16 of the Treaty on the Functioning of the European Union.

[56] CH suggested adding ",as far as possible,".
[57] OJ L 335, 17.12.2011, p. 1.

(76) In accordance with Articles 2 and 2a of the Protocol on the position of Denmark, as annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not bound by **the rules laid down in** this Directive or subject to **their** application **which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the Treaty on the Functioning of the European Union**. Given that this Directive builds upon the Schengen acquis, under Title V of Part Three of the Treaty on the Functioning of the European Union, Denmark shall, in accordance with Article 4 of that Protocol, decide within six months after adoption of this Directive whether it will implement it in its national law.

(77) As regards Iceland and Norway, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis[58].

(78) As regards Switzerland, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen acquis[59].

(79) As regards Liechtenstein, this Directive constitutes a development of provisions of the Schengen acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis[60].

---

58 OJ L 176, 10.7.1999, p. 36.
59 OJ L 53, 27.2.2008, p. 52.
60 OJ L 160 of 18.6.2011, p. 19.

(80) This Directive respects the fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaty, notably the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on these rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

(81) In accordance with the Joint Political Declaration of Member States and the Commission on explanatory documents of 28 September 2011, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition instruments. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

(82) This Directive should not preclude Member States from implementing the exercise of the rights of data subjects on information, access, rectification, erasure and restriction of their personal data processed in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure.[61]

[61] ES objected that the draft text did not contain any specific elements providing special protection to children. In consequence ES suggested to include specific references to children being victims or even from the perspective of vulnerable people.

CHAPTER I
GENERAL PROVISIONS[62]

Article 1

Subject matter and objectives[63]

1. This Directive lays down the rules relating to the protection of individuals with regard to the processing of personal data[64] by competent public[65] authorities[66] for the purposes of[67] the prevention[68],

---

62 PL, FI, UK scrutiny reservation on Chapter I. SI critical to Chapters I and II. Cion scrutiny reservation on the text in bold in Chapters I and II.

63 DE deplored the fact that the DPFD's basic philosophy of minimum harmonisation combined with a prohibition on 'data protection dumping' had been lost in this text. Cion explained that this proposal did not seek to attain full harmonisation, but at the same time went beyond the minimum harmonisation of the DPFD. Several Member States (AT, DE, NL and RO) stated that the exact nature of the harmonisation (minimum or maximum) the proposed Directive sought to attain was unclear. DE, UK required that it be set out that the Directive set out a minimum standard. In this context DE, supported by NL and CH, also deplored the fact that Member States would no longer be entitled to maintain stronger data protection requirements than those set by the proposed Directive (unlike what is the case under Article 1(5) DPFD). Cion affirmed, however, that it would still be possible for Member States to impose more stringent data protection rules (in particular purpose limitation) rules in specific cases and demand other Member States to comply therewith in case of transfer of personal data governed by these specific rules. DE said that it was important that the existing procedural powers were not altered or restricted by data protection rules. DE was of the opinion that the Commission's presentation of the administrative burden was insufficient. DE, NL and UK entered scrutiny reservations on the whole Directive. BE entered a substance reservation on Article 1.1. FI found that Article 1.1 did not clearly set out whether court activities were covered by the Directive. BE and UK reservation of substance.CY scrutiny reservation on Article 1.1. NO meant that the police authorities should be allowed to apply only one instrument**..**

64 SK thought that only automated forms of processing should be covered.

65 NL said that the police did not only investigate criminal offences, maintained public order, it also had jobs of administrative nature. FR supported BE, ES and UK. FR thought that a recital should be added to clarify this. NO said that private enterprises could be involved in this area, *e.g.* as processors. Cion said that the DPD was only applicable to competent (public) authorities carrying out activities listed in paragraph and where the same activities were carried out by a private enterprise the Regulation was applicable (see Article 21 and recital 16 in GDPR). The Cion indicated that the DPD was applicable to courts for criminal matters whereas for other courts the Regulation would be applicable FI meant that adding *public order and security* would facilitate the implementation of the Directive and the Regulation.

66 FR suggested the insertion of "the Member States"' before "competent authorities". EL wanted further clarifications of "competent authorities" in order to ensure that investigators and prosecutors were included. EE meant that "public authorities" created a misunderstanding if both the Regulation and Directive are applicable. Pointing to Article 2.2(e) in GDPR, EE thought that many bodies would be outside the scope of both the GDPR and the Directive. IT further suggested that specific rules be set out to indicate that private entities (subcontractors, outsourcers, cloud providers and contractors) should be considered joint controllers. If the private nature of such private entities was predominant provisions should ensure that they are governed by the GDPR, potentially with safeguards considered necessary under Article 21 of the Directive.

investigation[69], detection[70] or prosecution[71] of criminal offences and for these purposes, [72],safeguarding of public[73] security[74] or the execution of criminal penalties[75].

---

67 Cion stated that the notion of "public" had moved from the GDPR to the Directive and that the Cion was against applying the Directive to private bodies since that was against the logic of the Treaty.

68 FR wished certain activities carried out by the special administrative police aiming at prevention of an offence or unrest against national security to be covered by the Directive. DE wanted that threat prevention by the police be covered by uniform provisions.

69 NO meant that is was difficult to distinguish between police and criminal investigation in cross-border cases.

70 PL suggested to add "of crime and perpetrators".

71 FI wanted that "prosecution" be clarified in particular to know whether courts and prosecutors are covered by this Article and if so to what extent. The Chair explained that courts are covered and that recital 55 had been changed to make this explicit. For EE "prosecution" covered both the pre-trial and trial phase and the same law applied in EE so where was the borderline for the Directive? FI wanted to a clarification of the exact coverage of the Directive in respect of *prosecution* and courts.

72 DE gave the example of the police being called to a house where a dead body has been found, if there has been a murder, *i.d.* a criminal offence the Directive would be applicable whereas if it is a natural death the Regulation would be applicable. A missing person is another example, this uncertainty would decide if the Directive or Regulation would be applicable. This situation was not satisfactory according for DE and EE. ES found it useful to discuss whether private security activities were covered and noted that only processing operations carried out by private security operators having a public purpose could be covered by the Directive. ES stated that it was necessary to look at the tasks and the function that were carried out and not by whom. Support from FR. DE further said that problems arise due to the fact that the 95 Directive will be replaced by a Regulation having for consequence that MS would not be allowed to transpose all the provisions from this Directive and GDPR into national law taking account of the national situation/context. ES and DE asked about "civil protection, and whether it was covered. For EE it was not clear to what authorities the Directive would be applied when they performed an activity not as their sole/predominant task. EE asked if for example law enforcement authorities would be covered and what about environmental offences. EE and CH did not find that the Directive should cover courts and judicial bodies. BE, supported by CZ, DE, RO, wanted to delete "for these purposes"; CZ meant that public order should be maintained for other reasons than prevention etc of criminal offences.

73 ES asked whether *citizens* security was covered with this drafting.

74 AT scrutiny reservation on *public* security and meant that although it had been used previously AT was uncertain if the meaning was the same. RO asked for clarifications of the notion of *public security* since in RO the notion of public order exists but no public security. In the same vein ES said that *public* security had a particular meaning within the ES Constitution and that it would be difficult to translate it for ES. RO meant that maintaining public security was a purpose in itself. FI supported the use of *public security.* BE, CY, EE and NL preferred to keep *public order* rather than *public security,* for *BE* because it meant that public security differs from MS to MS. UK found the notion of public security uncertain. FR preferred *public order* because it fitted into its national law. DE, supported by PT, meant that many MS seemed to have problems with the notions *public order* and *public security* and as a consequence the scope became unclear. Cion preferred *public security* because it was a well-known notion in the acquis and was an autonomous definition.

1a. This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive[76] for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent public authorities.[77]

2. In accordance with this Directive, Member States shall:

(a) protect the fundamental rights and freedoms of individuals and in particular their right to the protection of personal data; and

---

75 BE, DE, ES, FI, FR, PL and SE, queried whether this Directive would cover court proceedings (also valid for Article 3(14). ES did not want the Directive to cover court activities. RO, supported by CZ, wanted to add "and ensuring public order and security". BE wanted to ensure that both arms/branches of the police were covered by the Directive. BE also wanted to insert a recital with the following wording: "the criminal character of the offences in Article 1 is not decided b y the Member States' national law but by the European Court of Human Rights which specifies that the criminal character depend on the following criteria; the severity of the potential crime that the person concerned risks to meet/face". EL wanted to know whether the processing of personal data in criminal records was included. RO suggested to exclude police activities linked to the operational side of the activity regardless of how they are classified in the MS national legislation. RO further considered that the maintenance of public order/risk represented a significant part of police work and that there were no clear distinction between the scope of GDPR and the Directive. RO meant that this had negative repercussions on other aspects of public order. Since the Directive will apply to domestic processing DE wanted to know what was meant with domestic data processing. IT asked for clarifications on the notion of competent authorities for the purposes …penalties " in order to precisely define the scope of the Directive and the interaction between the Directive and the Regulation. IT said that since it was difficult to distinguish tasks relating to those activities from purely administrative tasks it was necessary that the Directive and the GDPR be as consistent as possible. AT was in favour of extending the scope to the maintenance of public order as long as they fall within the ambit of EU law and therefore suggested the following addition to paragraph 1 after penalties and having deleted the text in square brackets "Public authorities in the sense of the Directive are the authorities established in the respective Member State, insofar as they are competent for the prevention, investigation, detection or prosecution of criminal offences or for the execution of criminal penalties."

76 SE and DE welcomed the new Article 1.1a but thought that a full stop could be put after "Directive".

77 AT, CH, DE, DK, ES, NL, SE and UK suggestion. CZ supported that MS could provide higher safeguards.. Cion welcomed the insertion of the paragraph as long as the free flow of data was not hampered.

(b) ensure that the exchange of personal data by competent public authorities within the Union is neither restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data. [78] [79] [80] [81] [82] [83]

[78] CZ and DE queried whether, *a contrario*, the respect for other existing rules could still limit the exchange of personal data. Reference was made, by way of examples, to the rules contained in the so-called Swedish Framework Decision. Cion stated these rules could still be applied. Cion also clarified that the proposed Directive would not affect Member States' competences to lay down rules regarding the collection of personal data for law enforcement purposes. DE wanted to know if this drafting meant that different levels of data protection can no longer be invoked as an acceptable argument for prohibiting or restricting the transfer of personal data to another MS. SE meant that the meaning of paragraph 1.2(b) and its effect for MS needed to be clarified. SE, supported by CH, DE, RO said that Article 1.1a and 1.2(b) seem to contradict each other. In contrast, EE saw no problems with paragraph 2.

[79] SK suggested to reformulate this paragraph as follows: "not restrict nor prohibit the exchange of personal data by competent authorities within the Union if individuals data protection is safeguarded". SE meant that the balance between individuals' integrity and security needed to be ensured and that aspect was not yet sufficiently clear in the current text.

[80] IT and SI queried the interaction with other fundamental rights and referred to the need to protect attorney-client privilege. CH suggested to insert a recital to clarify that MS could foresee more restrictive provisions with regard to the purpose for which data could be used.

[81] DE sugg: p.10 in 14901/2/13 rev 2. Cion meant that new Article 7a covered this.

[82] DE suggested to add "by restrictions or prohibitions stricter than those applicable at national level."

[83] ES suggested to let current (b) become (c) and add the following text under new paragraph "b) ensure that the treatment of personal data by the competent authorities let them perform efficiently their legal duties as regards the detection, prevention, investigation or prosecution of criminal offences, [the maintenance of public order,] or the execution of criminal penalties".

Article *2*

Scope [84]

1. This Directive applies to the processing of personal data by competent public authorities for the purposes referred to in Article 1(1). [85]

2. This Directive applies to the processing of personal data wholly or partly by automated means[86], and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[87]

[84] BE, CZ, DK, AT, ES, UK considered that the delimitation of the scope of this Directive and the one of the GDPR was not sufficiently clear (*e.g.* when the police is using the same personal data in different situations). UK wanted that the scope be limited to personal data that are or have been transmitted or been made available between MS. EE scrutiny reservation.

[85] BE scrutiny reservation on the new drafting. CZ, DK, RO, SE, SI and UK were of the opinion that the regulating of national processing of personal data by competent authorities in the area of law enforcement and criminal justice was not in conformity of the principle of subsidiarity. It requested a thorough analysis of ". by the MS when carrying out activities which fall within the scope of Union law" as set out in Article 16 TFEU. DE, supported by AT, suggested to add in the end of the sentence: "Article 1(1) and their transmission by competent public authorities for other purposes.". CZ pointed to Declaration 21 annexed to the Lisbon Treaty setting out that specific rules may be necessary for the protection of personal data in the fields of judicial cooperation and police cooperation and concluded that national processing of such data should not be covered by the Directive. DE said that data may need to be transmitted for other reasons, *e.g.* a school needed to be informed about young offenders, asylum or data may need to be passed on to concerned persons.

[86] HU considered that the distinction of data processing by automated means and other means seemed to run counter to the goal of a consistent data protection legislative framework. HU suggested to delete the words "whether or not by automated means" or as a alternative to deletion to add: "irrespective of the means by which personal data are processed,".

[87] DE scrutiny reservation. DE queried whether files as well as (electronic) notes and drafts are covered by the scope of the Directive. DE considered that if the scope covers all three forms, exceptions are necessary not to overburden the authorities.

3. This Directive shall not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law[88]; (…)[89]
[90]

[88] AT, ES and IT thought this required clarification. ES and IT referred to the difficulties of distinguishing between criminal intelligence and national security intelligence operations. IT referred to specific case of personal data collected in the context of foreign security (CFSP) operations, which might be transferred to law enforcement authorities. IT asked for clarification as to what activities carried out by which bodies are considered outside the scope of Union law, possibly including an indicative list. Cion, supported by UK, thought it was not expedient to define the concept of national security in secondary legislation as this concept is used in the TEU. DE meant that at least public security requirements were needed. FR suggested to insert the following: "by the MS when carrying out activities under chapter 2 of title V of the TFEU." FR considered also that it was necessary to change recital 15 in line with what was already done in GDPR. AT suggested the following addition to paragraph 3(a) " such as an activity concerning national security, or an activity which is not governed by legislative measures in the area of judicial or police cooperation based on Title V Chapters 4 and 5 (Art. 82 – 89) TFEU". The Chair said that it was clear by the definition that the EU Treaties were excluded and that it was not necessary to set out all excluded areas. AT wanted that the content of "EU law" was clarified. NO said that as a non-member of the EU national security was not covered and that should be set out explicitly.

[89] DE meant that the deletion of "national security" was contra productive and that it was better to reinsert the text of the initial proposal relating to national security. Support from AT, FI, EE, NO and UK, for FI even despite recital 15. FI scrutiny reservation on its deletion.

[90] FR suggested to add the following point (aa) to paragraph 3: " (aa) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;". The FR wording used the wording as in GDPR, and recital 15 should be changed accordingly.

(b) by the Union institutions, bodies, offices and agencies[91].

[92]

[91] Many MS (CZ, DE, EE, ES, FI, LV, PT, RO, SE) queried why these bodies and agencies had been excluded from the scope of the Directive. AT thought the data protection regime of these bodies and agencies should be governed by a separate instrument. AT therefore suggested to add "such as Europol or Eurojust". Cion confirmed that it would, at a later stage, table a proposal to amend Regulation 45/2001 in order to align the data protection regime for Union institutions, bodies, offices and agencies align the data protection. DE thought this exclusion was difficult to reconcile with the Cion's stated aim of full harmonisation. BE reservation. The Chair explained that Europol, Eurojust and Prüm have their own regime of data protection. HU and RO asked how consistency between Europol, Eurojust and Prüm and GDPR and DPD could be ensured. Cion said that even if the text "Union institutions … agencies" was deleted the Directive could not apply to such bodies because a Directive can only apply to MS. Concerning consistency when proposing changes to Directive No 45/2001 the Cion would look at that. IT wanted that the relationship between Article 2(3)(b) and Article 59 be made clear.

[92] FI suggested the insertion of the following paragraph "(4) This Directive does not apply to personal data contained in a judicial decision or to records processed in courts during criminal proceedings." to ensure that national rules on judicial proceedings were not affected. For ES it was important that MS remain competent to legislate on the protection of personal data in matters that could affect national security or impinge on it in some way. If such competence was not set out in the Directive ES suggested to add a new paragraph (c) with the following wording: "c) concerning terrorism, organized crime and situations of serious disturbances to the democratic social order.". ES scrutiny reservation on national security. DE pointed to the RO text referring to its suggestion for Article 2.1 in GDPR "and for the purposes of maintaining and assuring the public order" (doc 8208/13).

Article 3

Definitions[93]

For the purposes of this Directive:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly[94], in particular by reference to an identifier such as a name, an identification number, location data, online identifier[95] or to one or more factors specific to the physical, physiological, genetic[96], mental[97], economic, cultural or social identity of that person. [98];

(…)

---

93 DE scrutiny reservation. EL, supported by DK, SE and UK, insisted on the need to ensure consistency between the definitions in this instrument and the GDPR, for IT uniformity of application was also important. FI and HU wanted to review the definitions once they had been more formalised in GDPR. ES meant that some positive progress had been made to align this instrument with GDPR but that *e.g.* controllers was particular for the Directive. Cion also welcomed the alignment with the GDPR. UK, supported by IE, thought that a definition of *consent* should be inserted in Article 3 as a possible legal ground for processing. In contrast IT did not approve the idea of a definition of consent. CH noted that in the draft for the modernised Convention 108 consent is legal basis for processing. Cion set out that consent was a legal ground in the 95 Directive and GDPR but thought that it should not be a legal basis for processing in the context of the Directive. Cion meant in the DE examples of blood sample or DNA testing consent was not the legal basis it was the law that required it; it related to consent to the measure. SI agreed with Cion that in law enforcement there was no such thing as a free consent.

94 DE wanted to reinsert the reference to "by means reasonably likely to be used" as set out in the Cion proposal should be reinserted into the body of the text. DE asked who should be able to identify the person. FR suggested inserting the following: "If identification requires a disproportionate amount of time, effort or material resources the natural living person shall not be considered identifiable".

95 FI and EE requested clarification of this concept and though that it should be complemented by the words "on the basis of which the data subject can be identified". UK queried whether the proposed definition would prevent law enforcement authorities from releasing personal data from unidentified suspects.

96 FR reservation.

97 FR and RO wanted to know what *mental* meant.

98 FR thought the definition from the 1995 Directive was better. SE queried whether the following data should be listed here: genetic, cultural or social identity of that person. UK thought the definition was not sufficiently technology-neutral. FI suggested to align this definition to the one in the GDPR. FR said that DE

(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination (…)[99] erasure or (…)[100];

(4) 'restriction of processing' means the marking[101] of stored personal data with the aim of limiting their processing in the future; [102]

(5) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis; [103]

---

[99] HU opposed the deletion of *restriction*.

[100] FR reservation because of the broad scope of the definition. FR wanted to know if the mere presence of personal data implied automatic processing. DE wanted to reinsert *destruction* and add "blocking" instead of restriction. HU opposed the deletion of *destruction.*

[101] CH and FR said that the texts uses the word *restriction of processing* but in reality it was about *blocking* and that should be made clear in the text. CH, DE, EE, HU, NO, NL and SI preferred the word *blocking* as is used in DPFD.

[102] RO asked for clarifications on the meaning of *restriction. C*ion explained it thought this term was less ambiguous than the term 'blocking', which is used in the DPFD. DE and SE did not see the need for a new definition. Alternatively, SE and CZ suggested to define the term "marking" instead of "restriction of processing". CZ reservation. DK found the definition unclear. SE wanted to delete "in the future" because the limitation applies from the outset. FR found the definition superfluous and wanted to delete the whole definition

[103] DE, HR and RO wanted to know whether paper-based criminal files (assembled by the police and or courts) were included in the definition. AT meant that it should be clear under which circumstances file in paper format fall under the Directive and referred to recital 15 in DPD.

(6) 'controller' means the competent public authority, which alone or jointly with others determines the purposes (…) and means[104] of the processing of personal data; where the purposes (…) and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law[105];

(7) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller[106]

[104] Cion considered that the references to *purpose* and *means* was the appropriate solution and ensured consistency with GDPR.

[105] UK though that the distinction between processor and controller was blurred here. ES pointed out that if private sector bodies are included in the scope of the Directive this will impact the definitions of *controller* and *processor.* Cion said that processing would be set out by law and that judges and prosecutors were not controllers because they were bound by the procedure law. SI asked if the prosecutors office was the controller since the individual prosecutor was not a controller. Following up on that, DE while pointing to Articles 11, 12, 15 and 16 which related to controllers required a clarification as to who would carry out these tasks. Cion suggested to clarify that in a recital. CY meant that the definition was moving in the right direction.

[106] PL scrutiny reservation. PL queried what this definition implied for transfers of personal data from the private to the public sector.

(8) 'recipient' means a natural[107] or legal person, public authority, agency or any other body other than the data subject, the controller or the processor to which the personal data are disclosed[108];
[109]

(9) 'personal data breach' *m*eans a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed[110];

---

[107] CZ, DE was opposed to the inclusion of natural persons in this definition, as only the authority which receives/processes personal data should be considered as recipient, not the individual working at those authorities.

[108] FR thought this definition was too broad as it would also cover data protection authorities. FR also suggested to include *third parties to whom data are disclosed* as in the definition of recipient in the 95 Directive. HU suggested the following addition: "… body "*other than the data subject, the data controller or the data processor*" to which …" or alternatively to delete the following from the definition: "natural or legal person, public authority, agency or any other body" and replace with: "third party". In consequence add a definition on "third party" as follows: " 'third party' means a natural of legal person, public authority, agency or nay other body other than the data subject, the data controller or the data processor".

[109] DE asked to insert a definition of "consent of the data subject" with the following wording: *"(8a) 'consent of the data subject' means any indication of wishes in the form of a declaration or other unequivocal act made without coercion in a specific instance and in the knowledge of the facts by which the data subject indicates that he consents to the processing of his personal data' ;"* CH agreed on that need of a definition on *consent* but suggested the following wording: *'the data subject's consent" means any freely-given specific, informed and explicit indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him being processed';"* Support from NO, BE and SI to set out a consent as a legal basis for processing; for SI in exceptional specific cases. Support from ES, AT, HU and RO to include a definition of consent. The Chair said that since consent was no legal ground for processing it was not necessary to have a defintion of consent. Cion said that it could not see the context where consent would be necessary and queried if a consent could be considered given "freely" in a criminal situation.

[110] Cion explained this definition featured already in the E-Privacy Directive. AT asked to clarify whether these breaches were limited to technical security breaches (Article 27) or also covered other personal data breaches. FR reservation: queried why the reference to third parties had been deleted. DK found the definition unclear. HU suggested the following changes to the definition: delete "security" and replace with "*the provisions of this Directive* leading to *any unlawful operation or set of operations performed upon personal data such as"* …because data breaches were not only linked to security breaches.

(10) 'genetic data' means all personal data, (…) relating to the genetic characteristics of an individual that have been inherited or acquired,[111] resulting from an analysis of a biological sample from the individual in question; [112]

(11) **(....)** [113];

(12) 'data concerning health' means (…) data related to the physical or mental health of an individual, which reveal information about his or her health status[114];;

[111] AT suggested to delete the text from *acquired.* For AT it was important that the genetic data was protected from the beginning of its existence. AT suggested an alternative(preferred) wording: "10. 'genetic data' means all personal data, of whatever type, concerning relating to the genetic characteristics of an individual that have been inherited or acquired, in view *of* an analysis of a biological sample from the individual in question which are inherited or acquired during early prenatal development"

[112] FR reservation. AT scrutiny reservation. AT worried that 'genetic data' and "biometric data" receive special protection. DE suggested adding "non coding DNA sequences are not regarded as genetic data". NO, SI wanted to delete the paragraph.

[113] PL remarked that biometric data could be used both to verify and to identify persons. CH, DE, SI and SE suggested to remove paragraph 11. CH and SE said that the Directive did not contain any other provision on processing of *biometric data*. Cion could accept to delete the definition.

[114] FR thought that the level of protection afforded to personal data should be proportionate to the importance thereof. CZ, DK, SE and UK thought the definition was too broad. Cion scrutiny reservation.

[(12a) 'profiling' means any form of automated processing of personal data intended to create or use a personal profile by evaluating personal aspects relating to an individual;[115]]

(…)

[116]

(14) 'competent public[117] authority' means [118]any (...)authority[119] competent for the prevention, investigation, detection or prosecution of criminal offences, and for these purposes[120], safeguarding public security or the execution of criminal penalties [121];

---

115 Cion reservation. DE scrutiny reservation. FR, supported by NL, RO, suggested to use the definition in the CoE recommendation from 2010 on profiling. SI wanted either to use the definition in GDPR or the one in the CoE recommendation.

116 DE considered it necessary to insert a definition of *criminal offence* with the following wording: (**12b**) *'criminal offence' covers all infringements of the rules of law which are punishable under national law, provided that the person concerned has the opportunity to have the case tried by a court having jurisdiction in particular in criminal matters.* Cion did not see the need for such a definition since it was a standard term.

117 DE scrutiny reservation.

118 DE thought that it might ne necessary to reword paragraph 14 once Article 1(1) had been agreed.

119 FI welcomed the insertion of *administrative and judicial* before *authority.* FR thought that the definition included private entities and did not approve of that but preferred *public authorities.* NL raised concerns about the administrative/judicial authorities and the activities of police forces and the links with Article 1.1.

120 RO and UK suggested to delete *for these purposes.*

121 Cion scrutiny reservation, linked to the authorities being covered by the definition. PL remarked that courts were excluded from this definition. PT thought this definition served little purpose. DK queried whether *e.g.* surveillance authorities were covered by this definition. FI stressed that courts were not covered by this definition. IT thought that the definition could be improved by saying for example: "authority on which national legislation confers the competence to …" or "institutionally competent to…". BE suggested to add "and the prevention of danger." EE said that it had the same concerns as indicated for Article 1.1 and, supported by DE, that, in addition, paragraph 14 did not follow the same logics as in Article 1.1. CZ said that the whole definition was different and that the Directive should be applied to ordinary courts. IE and IT expressed concerns about this paragraph. Cion said that courts and prosecutors should be covered by the Directive.

(15) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 39.

122

122 CH suggested to add a definition of consent in line with the drafting in Article 4.8 in the draft GDPR: " 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;" (doc 6828/13) HU suggested inserting a definition from the general approach on a draft Directive on the use of PNR data for the prevention. detection, investigation and prosecution of terrorist offences and serious crimes: " 'depersonalising through masking out of data' means rendering certain data elements of such data invisible to a user without deleting these data elements". (8916/12) IT opposed the insertion of consent because it meant that consent cannot be the legal basis for processing in the field covered by the Directive.

CHAPTER II [123]

PRINCIPLES

Article 4

Principles relating to personal data processing[124]

1. Member States shall provide that personal data must be:

(a) processed (…) lawfully and fairly;[125]

(b) collected for specified, explicit and legitimate purposes and not further processed[126] in a way incompatible with those purposes[127];

---

123 FI, PL, UK scrutiny reservation on Chapter II. Cion scrutiny reservation on the text in bold. SI critical to Chapters I and II.

124 PL scrutiny reservation. AT and DE deplored the apparent absence of the requirement of data minimization. DE thought that a number of important requirements from the DPFD, e.g. the requirement that the data must be processed by competent authorities, purpose limitation, are lost in the proposed Directive. DE further stated that provisions on archiving, setting time limits for erasure and review are missing. SE queried why Article 3(2) DPFD had not been incorporated here. Cion affirmed that it did not intend to lower the level of data protection provided for under the DPFD. EL considered that the same requirements as in Article 5 of the GDPR should be set out. UK considered that the draft Directive should be a minimum standards Directive and in consequence wanted to retain the wording in Article 3 of the DPFD. CH also preferred Article 3.2 of DPFD and AT preferred the text as proposed by Cion.

125 HU suggested to add "and to the extent and for the duration necessary to achieve its purpose" in the end of paragraph (a) or add a new paragraph (bb) "processed only to the extent and for the duration necessary to achieve its purpose." EE and SE scrutiny reservation on the reinserting of *fairly*. DE opposed to the reinsertion of *fairly*. IE, supported by SI, saw problems in reinserting *fairly* and pointed to covert police investigations that would not be possible then. SI meant that future proceedings would be influenced and meant that *fairly* had nothing to do in Article 4. CY asked whether it was feasible to ensure fairness. FR and NL and Cion on the other hand welcomed *fairly* and FR saw no problems with police activities if the term was reinserted.

126 EE meant that *further processing* was the most complicated in this Article.

127 It was not clear for DE and SE how Articles 4 and 7 were linked, in particular as regards *purpose limitation.* NL meant that the *further processing* was not resolved here.

(c) adequate, relevant, and not excessive in relation to the purposes for which they are processed[128];

(d) accurate and, where necessary[129],, kept up to date; (…)[130]

(e) kept in a form which permits identification of data subjects[131] for no longer than is necessary for the purposes referred to in Article 1(1);[132];

(ee) processed in a manner that ensures appropriate security of the personal data[133].

(…)

[134]

[128] DE thought the DPFD was clearer. PT also queried about the use of personal data for other purposes.

[129] EL, NL suggested to delete "where necessary".

[130] CH, supported by NO, RO, suggested the following wording for (d): "(d) accurate and, where possible and necessary**,** completed or kept up to date; (…)"

[131] SE, supported by BE, wanted to delete the words "in a form which permits identification of the data subject" since data that does not allow identification of persons is not personal data.

[132] DE queried about rules on archiving on judicial decision. UK meant that this paragraph undermined future investigations. EE said that this paragraph was problematic for EE; how could personal data be deleted from data collected in criminal proceedings and when could data be archived? EE asked what point in time paragraph (e) referred to. EE meant that future identification was problematic. HU suggested to add that the personal data must be "processed lawfully and to the extent and for the duration necessary to achieve its purpose". CH suggested replacing (e) with the following text from Article 4(2) DPFD: "(e) erased or made anonymous when they are no longer required for the purposes for which they were lawfully collected or are lawfully further processed.; "IT wanted to link the period for which data can be kept with the objectives of the Directive and with the purposes for which the personal data was collected. SE found that the scope for further processing was narrowed down with the addition of the reference to Article 1.1 and suggested to delete that reference. Also UK raised concerns about the reference to Article 1.1 and meant that it would cause difficulties for future investigations. Cion on the other hand accepted paragraph (e).

[133] DE asked whether paragraph (ee) was purely declaratory or if it went further, if so it should be made clear.

[134] AT suggested the insertion of a new paragraph 1a with the following wording: "1a. Personal data shall be erased or made anonymous when they are no longer required for the purposes for which they were lawfully collected or are lawfully further processed. Archiving of those data in a separate data set for an appropriate period in accordance with national law shall not be affected by this provision." In addition AT pleads for the re-introduction of provisions along the lines of Article 4.3 and 4 of DPFD.

2. The controller shall be responsible for compliance with paragraph 1. [135]
[136]

[135] DE asked whether the amended text was meant to change the content.

[136] BE, CZ, EE, IE, NL, NO and UK wanted to insert a paragraph 3 with the following text from Article 3(2) DPFD: "3. Further processing for another purpose shall be permitted in so far as: (a) it is not incompatible with the purposes for which the data was collected; (b) the competent authorities are authorised to process such data for such purpose in accordance with the applicable legal provisions; and (c) processing is necessary and proportionate to that other purpose. The competent authorities may also further process the personal data transmitted by the competent authorities of other Member States for historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as making the data anonymous." CH supported the text until (c) and the text "to that other purpose". CH noted that the reference in paragraph (3) would in consequence be to "paragraphs "1 and 2". EE support for further processing for statistical purposes. FR favoured the insertion of a reference to historical/statistical or scientific purposes but queried about the links to Article 7.2 and wanted to ensure duplication of provisions. The Chair pointed to recital 20 concerning statistical purposes. Cion agreed with BE and FR also concerning the links to Article 7.2.
SE supported the inclusion of the reference to "historical, statistical or scientific" purposes. IE wanted to add provisions permitting further processing in line with article 3.2 in DPFD; "competent authorities are authorised to process such data for other purpose in accordance with the applicable legal provisions" and "processing is necessary and proportionate to that other purpose".

137 138

137 DE suggested to insert a new Article 4a with the following wording:
"Article 4a
Rectification, erasure and blocking[137]

1. Personal data shall be rectified if inaccurate.**137**
2. Personal data shall be erased or anonymised if they are no longer required for the purposes for which they were lawfully collected or for which they are lawfully being processed**137**.
3. Personal data shall not be erased but merely blocked if[137]

(a) there is legitimate reason to assume that erasure would impair the data subject's legitimate interests;
(b) they have been stored for the purposes of backing up data or data protection supervision[137], or
(c) the erasure would be technically feasible only with a disproportionate effort, for instance on account of the special nature of the storage[137].

4. Without the consent of the data subject blocked data may only be processed for the purpose which prevented their erasure. They may, in individual cases, also be processed if, after weighing all the circumstances, the public interest in processing overrides the interest of the data subject standing in the way of the processing; in particular they may be processed, if this is essential for discharging the burden of proof.[137]
5. Appropriate time limits shall be established for the erasure of personal data or for a periodic review of the need for the storage of the data. Procedural measures shall ensure that these time limits are observed. ". DE noted that data that had been blocked could not be erased. FI expressed a positive view on the DE text, in particular paragraphs 3(c) and 4.

138 AT suggested to add a new Article 4a along the lines of Article 4a in the Droutsas report:
"Article 4a
Access to data initially processed for purposes other than those referred to in Article 1(1)
1. Member States shall provide that competent authorities may only have access to personal data initially processed for purposes other than those referred to in Article 1(1) if they are specifically authorised by Union or Member State law which must meet the requirements set out in Article 7(1a) and must provide that:

(a) access is allowed only by duly authorised staff of the competent authorities in the performance of their tasks where, in a specific case, reasonable grounds give reason to believe that the processing of the personal data will substantially contribute to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
(b) requests for access must be in writing and refer to the legal ground for the request;
(c) the written request must be documented; and
(d) appropriate safeguards are implemented to ensure the protection of fundamental rights and freedoms in relation to the processing of personal data. Those safeguards shall be without prejudice to and complementary to specific conditions of access to personal data such as judicial authorisation in accordance with Member State law.

2. Personal data held by private parties or other public authorities shall only be accessed to investigate or prosecute criminal offences in accordance with necessity and proportionality requirements to be defined by Union law by each Member State in its national law, in full compliance with Article 7a."

Article 5

Distinction between different categories of data subjects[139]

(…)

[139] Cion reservation against deletion. DK and SE welcomed the deletion and requested that the corresponding recitals to be removed. Contrary to this AT that wished to maintain both recitals 23 and 24.

Article 6

Different degrees of accuracy and reliability of personal data[140]

Member States shall provide that the competent public authorities shall ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, each competent public authority shall verify quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of data, available information shall be added which enables the receiving competent authority to assess the degree of accuracy, completeness, up-to-datedness and reliability.

(…)[141]

[140] HR found the text confusing and suggested dividing it in two parts. BE, CH, RO, SI and UK questioned the added value of the Article. FR and UK said that Article 4(d) set out the same idea. BE and CZ suggested to delete the Article. IE, supported by SE, suggested to use language from DPFD; IE questioned the need to have the Article at all. AT in contrast accepted the reinsertion of an Article with that heading. NL noted that the text was more tightly drafted than in DPFD and seemed more binding. NL asked to whom the Article was addressed. ES considered that the competent authorities and not the MS were the addressees of the obligation CZ could accept the DE suggestion for cross-border cases. ES asked why paragraph 8.2 of DPFD was not inserted. FI thought that an Article on accuracy was needed but was not certain that current Article 6 fulfilled that requirement. NO wanted it to cover also domestic processing. Cion declared that they were not against the text of Article 8 DPFD.

[141] DE, supported by CH and NO, suggested to insert parts of Article 8 DPFD: " The competent authorities shall take all reasonable steps to provide that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, the competent authorities shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of data, available information shall be added which enables the receiving Member State to assess the degree of accuracy, completeness, up-to-datedness and reliability." . ES and UK saw merits in this suggestion and UK the qualifier *reasonable steps.*

Article 7[142]

Lawfulness of processing[143]

1. Member States shall provide that the processing of personal data is lawful[144] only if and to the extent that processing is necessary[145]:

[142] CH, DE and SI scrutiny reservation. DE considered it unacceptable that only the general lawfulness in Article 7 would apply to further processing of data previously transferred within the EU. In its opinion this would mean that data protection law aspects would take precedence over police and/or criminal procedural law. FI wanted to insert this Article after Article 4. ES said that since Article 3 did not define consent it was not clear why this was not addressed in this Article and pointed out that consent was important for alcohol tests for example. ES meant that a reference to consent would give added value to the Article and would provide an additional guarantee. AT, FR, HR and IE favoured the addition of consent. SI suggested to introduce a recital on consent. CZ suggested to build in consent for processing, *e.g.* victims of stalking could consent to have phone calls tapped. FR meant that consent had to be treated with caution and did not want to have it as an autonomous legal basis for processing. BE meant that consent set out in a law would be acceptable. BE reservation on consent. Cion agreed that text on consent could be set out for example in a recital clarifying that in some cases consent could be a relevant factor. Cion questioned whether consent was necessary beyond what was set out in paragraphs (c) and (d) and stressed that consent should not be an individual ground for processing.

[143] BE, DE and FR pointed to the difficulties to delimit the scope of the GDPR and this draft Directive. SE claimed that the Article was too restrictive. UK recommended to delete this Article since the minimum standards set out in the DPFD were both sufficient and appropriate for fundamental rights protection. DE said that it was impossible to agree to this Article until the exact scope of the Directive was decided. DE meant that it was necessary to explain how Article 7 and 4 are to be read, in particular the principle of purpose limitation. FR suggested to remove the Article due to a duplication with Article 4(a). SI said that lawfulness was set out in Article 4 and was therefore dubious about the need of Article 7. FR meant that Articles 7 and 1.1 were contradictory and if the Article 7 had to stay it was necessary to clarify the links between the two Articles. DE meant that deleting Article 7 would not solve any problem and that Article 4 and 7 were linked.

[144] IE questioned if lawful processing always was fair and wanted to add a new "recital/provision" setting this out.

[145] CH, IE and UK wanted to provide for consent from the data subject, DK could consider it. IT and PT questioned the possibility of consent in the field of police work. FR reservation as regards consent. Cion confirmed that consent was not relevant in the field covered by the draft Directive. DK wanted to keep the scope broad enough for competent authorities' processing.

(a) for the performance of a task carried out by a competent public authority, based on Union law or Member State law[146], for the purposes set out in Article 1(1); or

(…)[147]

(c) in order to protect the vital interests[148] of the data subject or of another person[149]; or

[146] DE, supported by RO, meant that is was difficult to attain the purpose of the Directive if the reference was made to national law which was correct since law for the police and criminal as well as criminal procedure law remain a national competence. DE also queried about what would happen to internal EU data processing.

[147] DE and SE wished to reintroduce paragraph (b)for DE to read as follows: " for compliance with a legal obligation or for the lawful exercise of a legal power the controller is subject to". For DE for lawfulness for practical and legal reasons namely that data protection law must follow specialized law on the police and judiciary (which lies within the competence of the Member States) and not the reverse. In DE provisions for the transmission of information from the police or judiciary to other authorities are not set out in law so to cover such cases the reference to *legal power* is necessary. DE was considering whether a material restriction should be inserted in (b) which could be worded as follows: "The statutory provision must pursue an aim which is in the public interest or necessary to protect the rights and freedoms of third parties, must safeguard the essence of the right to the protection of personal data and must stand in appropriate relation to the legitimate purpose pursued by the processing."
For SE it was for the sake of the principle of public access to official records that point (b) had to be reinserted.

[148] PL questioned whether economic or commercial interests were covered Cion indicated that only life or death situations were covered. SE queried about a definition of "vital" interests, in this Article as well as in Article 8.2 (b). HR suggested to replace *vital interest* with "life and physical integrity" of the data subject because HR meant that data should be processed also when it was necessary for the protection of the physical integrity of any person.

[149] DE scrutiny reservation. DE compared this Article with Article 1.2b of DPFD (protection of fundamental rights and freedoms of natural persons) and asked if Article 7 was the only restriction on MS when processing personal data. DE, supported by CH, also asked whether restrictions in national law would apply to the receiving MS when personal data was transferred/made available to them**.** DE considered it necessary to clarify whether this paragraph overlapped with paragraphs (a) and (b) and if that was the case paragraph (b) could be removed. DE said that if paragraph (b) and (c) were not overlapping it was necessary to determine if the Directive and/or Article 7.1 (c) was not to restrictive for a potential transmission to private parties. IT meant that paragraph (c) should be covered by paragraph (a) and should be attributed to the competence of the authority carrying out the processing.

[150]

(d) for the prevention of an immediate[151] and serious[152] threat to public security[153].

[154]

[150] ES suggested the insertion of the following paragraph: "d) to protect the freedoms and rights of the data subject or of another person and, in particular, to protect their interests as regards exercising legal claims,". ES considered that data processed by law enforcement officials are collected to provide authorities and citizens with information and data on incidents in general.

[151] IE asked whether it was possible to prevent an immediate threat and suggested, supported by HR, to replace "immediate" with "direct". CY, DE, DK, RO and UK suggested to delete "immediate", CY and RO to delete "serious" as well. DE considered that having both "immediate" and "serious" made the scope too narrow. CZ and SE suggested to replace "immediate" with "essential". ES suggested to replace "immediate" because this word is often misinterpreted and replace it with "direct" which is not temporal. For UK all threats to public security were important. Cion said that the text was standard wording in the acquis.

[152] IE meant that paragraph 1(d) was too narrow and therefore suggested to delete *immediate and serious* or to replace these words with *direct.*

[153] DE scrutiny reservation. DE said that the police must be able to take action even in the absence of of imminent danger therefore "immediate and serious" should be deleted. SI reservation. BE wanted to know if this was a reference to classical police work or something else. SI considered that Article 7 could be seen as limiting police work. SI suggested to add a new paragraph (e) "similar tasks might be added for additional tasks". NL thought that paragraphs (c) and (d) might be superfluous since these tasks are an obligation of the state. AT meant that what would not be covered by paragraph (d) would be covered by paragraph (a).

[154] ES suggested to insert the following paragraph: "(e) To protect other fundamental rights of the data subject or another person that deserve a higher degree of protection." DE, supported by HU, suggested the insertion of the following: "1a. In the cases referred to in paragraph 1 Member States may also provide that the processing of personal data is lawful if the data subject has consented to the processing." DE meant that Article 8.2 of the EU Charter sets out that personal data can be processed on the basis of consent and that consent-based data processing was essential in prevention projects such as taking blood or conducting DNA testing. DE meant that consent in these cases could be seen as alternatives to a court order.

2. Member States may [155] provide that the controller may for the purposes referred to in Article 1(1), further process personal data for historical, statistical or scientific purposes, subject to appropriate safeguards for the rights and freedoms of data subjects.[156]

[157]

[155] At AT CZ, CY, DE suggestion "shall" was changed to "may". FI welcomed the change whereas SE wanted to reinsert *shall.*

[156] UK queried why processing for historical or scientific purposes was different regarding law enforcement from other investigations. In the same vein, IE asked how historical purposes could fall within the scope of Article 1.1. SE said that the reference to Article 1.1 made it impossible to use for statistical purposes, SE therefore suggested to delete that reference. UK shared the view that data in law enforcement should not be treated differently when it came to the purposes set out in Article 7.2 and the reference should therefore be deleted. FR wanted to delete paragraph 2. SE wanted to see *archives* mentioned explicitly. AT could accept paragraph 2 and pointed at Article 11 last part that refers to *anonymous* data. DE was critical to the reference to Article 1.1 since it meant that the use of police data for historical, statistical and scientific purposes was not the normal field of use but meant that such use should be set out in the Directive and not in GDPR. FI meant that the reference worsened the situation for data for historical/statistical and scientific purposes. Cion declared itself willing to look for solutions.

[157] HU suggested to add a new paragraph to Article 7 as follows: "2. The basis of the processing referred to in points (a) and (b) of paragraph 1 must be provided for in (a) Union law, or (b) the law of the State to which the controller is subject."

158

Article 7a

Specific processing conditions ***159***

1. Member States shall provide that where[160] Union law[161] or the national law applicable to the transmitting competent public authority provides for[162] specific conditions[163] **(...)** [164] to the processing of personal data,[165] the transmitting public authority shall inform the recipient to whom the data are transmitted about such conditions and the requirement to respect them.

---

158 BE suggested to create a Chapter IIA.

159 DE wanted to delete Article 7a and said that it should be seen in connection with the addition of Article 1(2) (b). FR considered that the text was unclear and that it did not have its place among the Chapter on Principles. CH, EE, NL, SK, PL, PT and SK scrutiny reservation. FR and SE reservation. HR suggested to add that the data subject's consent could be a valid legal basis for the processing of their personal data.

160 BE suggested to replace *where* with *when.*

161 NL asked what was meant with EU law.

162 BE suggested to delete *for.*

163 DE wanted to know what *specific conditions* was.

164 NL asked to what *specific circumstances* referred.

165 In order to create an uniformity of handling codes at EU level and for practical reasons, BE asked to insert "these conditions are set out in accordance with the Europol handling codes. The transmitting ..." BE suggested that the same adaptations be set out in recital 25a.

2. Member States shall provide that the transmitting public authority[166] does not apply conditions[167] pursuant to paragraph 1 to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters IV and V of Title V of the Treaty on the Functioning of the European Union other than those applicable to **similar national data transmissions**[168].

169

166 NL said that the notion of *transmitting authorities* was deviated from the language in the DPFD.

167 FI and NL noted that the DPFD uses *restrictions* whereas here it was *conditions*, and therefore wanted to know if it was intended to cover something else.

168 CH suggested to replace the last part of paragraph 2 with the following words. "similar national data transmissions". For CH it was important that national transfers and Schengen transfers be regulated by the same conditions, CH therefore suggested to use the same formulation as in DFPD Article 12(2).

169 BE, supported by FI, suggested to insert a paragraph 3 which came from Article 16.2 of DPFD with the following text: "3. When personal data have been transmitted or made available between Member States, each Member State may, in accordance with the provisions of its national law, ask that the other Member State does not inform the data subject. In such case the latter Member State shall not inform the data subject without the prior consent of the other Member State."

Article 8[170]

Processing of special categories of personal data

1. Member States shall prohibit[171] the processing of personal data revealing racial or ethnic origin, political opinions, religion[172] or philosophical beliefs, trade-union membership, and the processing of genetic data[173] or of data concerning health[174] or sex life[175].

[170] PL scrutiny reservation on Article 8. CZ, DK, SE and UK preferred the drafting of DPFD that was not formulated as a prohibition. DE found that an absolute prohibition on processing data in paragraph 1 was too far-reaching and impractical. UK generally preferred the drafting of the DPFD. DK meant that it was necessary to bring clarity to the text and further considered that it did not make sense to have a prohibition. SE pointed at discrepancies between the definitions in Article 3 on genetic data and biometric data and the text set out in Article 8 SE said that criminal science used results from analyses and that it was necessary to define methods for criminal investigation. SE said that law enforcement would be difficult if genetic data could not be used. SE added that distinguishing marks of a person could be covered by *sensitive data*. In conclusion, SE advocated a reviewing of Article 3 and 8 to make them balanced and consistent.

[171] DE, supported by IE, wanted to replace "prohibit" with "restrict".

[172] SE noted that in Article 12 of DPFD it says *religious* whereas in paragraph 1 it says *religion* and asked if this was intentional.

[173] AT scrutiny reservation on genetic data. HR considered that it was necessary to further analyse the processing of genetic data. SI saw problems with genetic data as was the case in the GDPR.

[174] EE asked as an example if setting out that someone was drunk was acceptable or if it was considered as health data.

[175] SE was of the opinion that many data was covered by paragraph 1 and that would make it difficult to legislate. PT wanted to reinsert the requirement of need, as in DPFD. DE, supported by PT, was against an absolute prohibition to process sensitive data. PT said that what is sensitive data was not an absolute notion. DE wanted to add "to the extent which is strictly necessary" at the end of the sentence. HR thought that processing concerning health and sex life should be allowed because in cases related to crimes against sexual freedom such personal data would be collected regularly. RO wanted to add "biometric data" to the category with a special character. FR, supported by NL, said that the notions did not correspond to those set out in the 95 Directive, nor in the DPFD or the Charter and opposed the terms used.

2. Paragraph 1 shall not apply where: [176]:

(a) the processing is authorised by Union law or Member State law which provides appropriate safeguards[177] for the rights and freedoms of the data subjects; or

(b) the processing is necessary[178] to protect the vital interests[179] of the data subject or of another person[180]; or

[176] SI and NL scrutiny reservation. CH considered the list of exceptions not sufficiently long, *e.g.* consent is missing or health. In contrast, PT considered that the list of exceptions was too long. CH also considered that Article 7(d) could be added to Article 8.2. DE considered it worth reflecting whether Article 8 could not be formulated as an anti-discrimination provision, like Article 21 of the EU Charter of Fundamental Rights. DK preferred the drafting of Article 6 in DPFD. Cion declared itself willing to reconsider the list of exemptions.

[177] AT, ~~and~~ DE and NL required examples of safeguards and EE, HR, IT, NL and RO asked for a clarification of what *safeguards* was. IT meant in this context that recital 26 could be modified to address this problem, suggesting text on procedural guarantees, technological or security safeguards.

[178] NL and SI inquired why "strictly" had disappeared from the text compared to Article 6 in DPFD. DE meant that it was still unclear what was meant with *appropriate safeguards*.

[179] SE and SK required clarifications of the notion of "vital interests". CZ wanted to replace *vital* with *essential.* DE FR and SE meant that *vital interest* was too narrow. HR suggested to replace *vital interest* with "life and physical integrity" so that data would be processed also when it was necessary for the protection of the physical integrity of any person".

[180] DE thought that paragraph 2(b) was too narrowly focused especially if the DE suggestion for paragraph 1 was not accepted.

(c) the processing (…) is necessary for the prevention of an immediate[181] and serious[182] threat to public security[183].

[184]

[Article 9]

[(…) Profiling (…)[185]

1. Member States shall provide that a decision based solely[186] on profiling which produces an adverse legal effect[187] for the data subject or severely affects[188] him or her (…) shall be prohibited unless authorised by Union or Member State law[189] to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject (…).]

---

[181] ES and UK wanted to replace "immediate" with "direct" and EE to delete it.

[182] IE meant that paragraph 1(d) was too narrow and therefore suggested to delete *immediate and serious* or to replace these words with *direct.*

[183] DE suggested to add "or" at the end and insert a paragraph (d) with the following wording: "(d) the data subject has consented to the processing". DE considered that the provision was too narrow, especially if the DE suggestion in paragraph 1 was not accepted.

[184] ES suggested to insert a paragraph with the following wording: "(d) the data subject has given his explicit consent". Support from CH, DK, HU and IE. CZ suggested a new paragraph with the following wording: "data which the data subject has published him/herself or agreed to by the data subject.". UK supported that processing would be acceptable if the data subject has consented or it had manifestly made public. BE suggested to insert a new paragraph with the following wording: "(d) the processing relates to data which are manifestly made public by the data subject." Cion said that it would consider these suggestions.

[185] RO suggested to define "profiling" and move the Article to Chapter III, support from CZ, EE, IT, FI, SI, SE to define "profiling". DE, ES, IT, SI entered scrutiny reservations. SE serious doubts about the Article. Cion reservation. DE meant that it was necessary to determine if Article 9 in its current form is covered by the legislative competence of the EU. CZ said that since there was no final agreement on the text on profiling in the GDPR it was not possible to decide the text for the Directive.

[186] FR asked for the deletion of the word "solely".

[187] EE asked who would assess the adverse legal effect and how.

[188] SI wanted to remove *severely affect* .

[189] FR wanted to know why the reference was to "a law" and not the generic "by law". FR, IT, PT and UK preferred *by law*, here as well as in the rest of the Directive.

CHAPTER III
RIGHTS OF THE DATA SUBJECT[190]

Article 10

Communication and modalities for exercising the rights of the data subject[191]

1. (…)

[190] SK scrutiny reservation on Chapter III. DK meant that the rights to information and to access did not reflect the specificities of the area covered by the Directive. IE believed that the rights in Chapter III should not be exercisable so as to permit access to a note made by a judge or a communication between judges exercising the judicial function i.e. notes made prior or in the course of a hearing, or in anticipation of giving judgment following a hearing in court proceedings. IE, supported by UK, therefore suggested the addition of a new provision to provide that Member States may adopt legislative measures exempting judges' notes and communications between judges exercising judicial functions from the rights and obligations set out in Articles 11, 11a, 12 and 15.

[191] BE referred to a text submitted by FR (DS 1850/12) and indicated that it preferred that text because it assumed the right to information and then set out the exceptions. Cion stated that as a principle according to Article 8 of the EU Charter of Fundamental Rights of data subjects has the right to access data concerning him/her but that exceptions could be set out to that right. Article 16 TFEU equally set out that right. UK agreed to have right of access as an exception and not as a rule**.** DE and SI scrutiny reservations on Article 10. BE asked whether the information to be provided was of a general or individual nature. LU meant that it was necessary to revise Article 10 to simplify the administration. The Chair noticed support for the deletion of paragraphs 1-3, in order to avoid information on every step; it should be enough to receive an outcome of the proceedings. The Chair also said that it could be considered to add "as far as possible" and add a recital also indicating that a translation into the official language would be enough. FR suggested to move Article 13 to become Article 10 and thus become the principle for the rights of data subjects, with the following wording: "*Article 10*

Rights of the data subject

1. In view of the specific nature of the purposes of processing defined in Articles 1 and 2 of this Directive, Member States may take any measure, necessary and proportionate in a democratic society, restricting the rights of individuals regarding their personal data:

(a) to avoid hampering administrative or legal inquiries, investigations or procedures;
(b) to avoid prejudicing the prevention, investigation, establishment and prosecution of criminal offences or the execution of criminal penalties;
(c) to protect public security;
(d) to protect the rights and freedoms of others.

2. Member States may determine categories of data processing which may wholly or partly be subject to the measures provided for in paragraph 1." The actual Article 10 would consequently be renumbered number 11 according to FR.

Referring to Articles 10, 11, 11a and 11b, AT meant that the right to information and to access has to be the rule.

2. Member States shall provide that the controller shall take appropriate measures to provide any information referred to in Articles 11 and 11a and any communication under Articles 12 and 15[192] and 29 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language[193]. The information shall be provided in writing , including where appropriate, electronically or by other means.[194]

3. Member States shall provide that the controller takes all reasonable steps to[195] provide the information referred to in Articles 11 and 11a and to facilitate the exercise of data subject rights under Articles 12 and 15 (…).[196]

[192] DE suggested to make the references to "Article 12 to 16 and 29"

[193] DE queried if the wording in Article 11.2 of the GDPR should be used in this paragraph. DE suggested to add "as far as possible" in the end of the sentence to clarify that translations are not required and since Directive 2010/64/EU contains comprehensive rules on translation obligations in criminal procedure.

[194] DE wanted to delete the last sentence since it is more practical that only refusals be in writing. ES supported that deletion because it would cause an excessive administrative burden. ES wanted the text to be set out in Article 11.

[195] FI wanted to delete the text from "provide the information" until "Articles 11 and 11a"

[196] FI considered this paragraph as over bureaucratic and questioned the need for it. CH, DE and EE and CH also found the paragraph superfluous and wanted it deleted. NL wanted the text to be drafted more tightly. SE wanted to know if the obligation concerned all individual steps or something else. Cion suggested to add paragraph 3 to Article 14.

197

4. In cases referred to in Articles 12 and 15, Member States shall provide that the controller informs the data subject in writing of any refusal or restriction of access, or of any refusal of rectification, erasure or restriction, of the reasons for the refusal and of the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy**.** [198].

197 DE wanted to insert a new paragraph 4a containing a generalized summary of Article 13.3 and 15.2 with the following wording: "4a. In cases referred to in Articles 12, 15 and 16, Member States shall provide that the controller informs the data subject in writing of any refusal or restriction of access, rectification, erasure or blocking, of the reasons for the refusal and of the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy. This shall not apply where the provision of such information would undermine a purpose under Article 13 (1)."

198 Some delegations (EE, FI, IT, NL)considered it useful to insert a concrete deadline. Others, like CZ, DK, SI was not in favour of a time limit. DE found the paragraph bureaucratic and queried if the data subject was really helped by all information on follow-up. LV also requested a clearer and more precise wording. RO wanted a clarification of what was meant with "undue delay". DE suggested to delete paragraph 4 in order to make it clear that it was not necessary to inform the data subject of every single step taken in response of his/her request.

5. Member States shall provide that the information provided under Articles 11 and 11a and any communication under Articles 12, 15[199] and 29 shall be provided (…) free of charge[200]. Where requests are manifestly unfounded or excessive,[201], in particular because of their repetitive character (…), the controller may refuse to act on the request[202]. In that case, the controller shall[203] bear the burden of demonstrating the manifestly unfounded or excessive character of the request (…)[204].

199 DE asked to insert Article 16 as well.

200 SE informed that data subjects had to pay a fee if they asked to have a lot of information but received information once a year free of charge. DE and NL scrutiny reservation. DE believed that the access rights of data subjects should not be undermined in fact by unreasonably high fees. NL asked whether it was reasonable to provide information *free of charge.* SE preferred the previous version of paragraph 5. DE noticed that the wording was different from the one in the DPFD. To avoid an increase in speculative requests and greater workloads, the UK suggested the following wording from the GDPR "On request and without an excessive charge, the controller shall provide a copy of the personal data undergoing processing to the data subject." UK considered that having the same drafting as in the GDPR would promote consistency between the two instruments. IE supported to replace "free of charge" with "without an excessive charge". IT supported the alignment with the GDPR. IT pointed to Article 12.4a of GDPR and how it could be availed of.

201 Delegations referred to the discussion on "excessive" requests in the draft Regulation (Article 12.4) and pointed to the need to align the two texts.

202 CH suggested to add "or may charge a fee".

203 DE suggested to add "state the reasons for the refusal" and delete the end of the sentence starting with "bear the burden…

204 DE worried about the costs involved and referred to Article 17 in the DPFD where the wording is "without excessive expense". CZ, NL also preferred the text in the DPFD. UK meant that certain requests were of such a size that it was too much of a burden intended deliberately to overburden the organisation through its sheer size and therefore suggested the following wording: "Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, or volume…" CZ suggested to revert to simple principles, cf Article 17 in DPFD, *at reasonable intervals.*

5a. Where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 12 and 15[205], the controller may request the provision of additional information necessary to confirm the identity of the data subject.[206]

[205] DE wanted to add "Article 16".

[206] CH suggested replacing paragraph 5a with the following text: "5a. Where the data subject intends to exercise his or her rights according to Articles 12 and 15, he or she has to prove his or her identity to the controller." EE found that paragraph 5a needed to be strengthened. SE found it important that the data subject could identify him/herself in an appropriate manner.

Article 11

Information to be provided where the data are collected from the data subject[207]

1. Subject to Article 11b, Member States shall provide that where personal data relating to a data subject[208] are collected from the data subject, the controller shall, at the time when personal data are obtained[209], provide the data subject with *at least* the following information:[210]

---

[207] BE asked about the links between Article 11 and 10.3. BE, CZ, DK, ES, LU, PL and UK were sceptical to the Article and were of the opinion that the obligation to inform the data subject was too wide and would entail heavy burden on the police. UK meant that a "Neither Confirm Nor Deny" provision was vital here. DK preferred the FR text (DS 1850/12) and did not find it reasonable that the controller have the same obligation to inform a person indicted in a criminal proceeding and a person whose name had been collected as a witness for example. BG, EE, ES, IT said that this obligation would increase the administrative burden. DE did not consider that the costs were proportionate to the usefulness of the information obligation. DE found that Article 11 had been improved with the removal of many of the obligations but that it was still to heavy, DE suggested to look at Article 16 in DPFD or that the information requirement be made optional. NO meant that it would not be possible for the police to implement this obligation. While seeing the need for Article 11, NL had doubts about its implementation. It also preferred Article 12 in the FR text (DS 1850/12). FI, NO referred to Article 16 in DPFD. SI was also sceptical and wanted to understand how the draft Directive could be applied. CZ and PT were of the opinion that general information was necessary. BG, IT, UK suggested to set out minimum standards only. SE pointed out that the changes compared to Directive 1995 and DPFD were considerable and the current text was too inflexible. The Chair noted that the question on the burden on law enforcement authorities and the balance with the data subjects' rights was still open.FR suggested to redraft the current Article 10 that has become Article 11 as follows: "*Article 11*
Modalities for exercising the rights of the data subject

1. Member States shall provide that the controller takes all reasonable steps to have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of the data subjects' rights.
2. The processing of personal data, where it falls within the scope of this Directive, shall not be subject to any obligation to inform the data subjects. Member States may nevertheless provide for this information where it does not prejudice the purposes of the processing.
3. Except in the cases provided for in Article 10, Member States shall provide that the controller takes all measures necessary to enable data subjects to exercise the rights referred to in Articles 13 to 16.
4. Member States shall provide that the controller informs the data subject about the follow-up given to their request without undue delay.
5. Member States shall provide that the information and any action taken by the controller following a request referred to in paragraphs 3 and 4 are free of charge. Where requests are vexatious, in particular because of their repetitive character, or the size or volume of the request, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the vexatious character of the request."

[208] SE wanted to delete "relating to a data subject".

[209] UK asked whether it was realistic to provide all the information at the time of obtaining them. UK, supported by DK, meant that it could be enough to read out the rights and inform about how to complain about the data being collected at that moment. DK referred to cases of shoplifting and minor offences where such an information obligation would be very heavy.

(a) the identity and the contact details of the controller and, if any, of the data protection officer[211];

(aa) whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data; and[212]

(b) the purposes of the processing for which the personal data are intended;

(c) (…)[213]

(d) (…) [214]

(e) the right to lodge a complaint to a supervisory authority (…).[215]

(f) (…)

(g) (…).

---

[210] BE considered paragraph 1 too burdensome (for *e.g.* mobile controls) and that it would cost a lot, BE therefore suggested to replace paragraph *chapeau* with the following text: "Subject to article 11b, Member States shall ensure that where personal data relating to a data subject are collected from the data subject, the controller takes all appropriate measures to provide the data subject with at least the following information:". BE suggested a new recital 30a to explain this.

[211] For the sake of consistency with the GDPR, CH suggested to replace from "and if any …officer with the following: "the controller may also include the contact details of the data protection officer if any;"

[212] BE and CZ suggested to suppress paragraph 1(aa) because of the burden and the cost of the obligation. CZ found the information in (aa) was superfluous.
EE thought that whether the provision is obligatory or voluntary depended on the evidence and that was linked to the criminal procedure.

[213] FI wanted to reinsert paragraph (c).

[214] FI asked to reinsert (d).

[215] EE meant that it was not for the SA to intervene here.

216

2. (…)

3. (…)

4. (…)

5. (…)

217

Article 11a

Information to be provided where the data have not been obtained from the data subject[218]

1. *Subject to Article 11b*[219]*, Member States shall provide that where personal data have not been obtained from the data subject, the controller shall provide the data subject with at least the following information:*[220]

216 HR suggested to insert a new paragraph h with the following wording: "(h) The legal basis for the processing of personal data in cases where the collection of such data is mandatory."

217 CH suggests to have the same solution as in Article 14(5) of GDPR, namely: "6. Paragraph 1 shall not apply where and insofar as the data subject already has the information."

218 Since providing the detailed information in this Article would be burdensome for the authorities HR suggested that such information should be provided at the request of the data subject. HR found it questionable that the controller *e.g.* police authorities should be required to inform the person to whom the data relates of the fact that such data is collected since it may jeopardize the interests of the criminal proceedings. SE thought that the exceptions to the right to information such as the ones set out in Article 11.2 in 95 Directive were missing. IT suggested to introduce a possibility to correct the information in Article11a. CH scrutiny reservation.

219 FI wanted to add *subject to Article* 13 to the text.

220 BE considered that paragraph 1 chapeau was too burdensome and costly and therefore suggested to replace paragraph 1 with the following text: "Subject to article 11b, Member States shall ensure that where personal data have not been obtained from the data subject, the controller takes all appropriate measures to provide the data subject with at least the following information:". As a consequence BE suggested a new recital 30a.

(a) the identity and the contact details of the controller [221] *and, if any, of the data protection officer;*

(b) the categories of personal data concerned;

(c) the purposes of the processing for which the personal data are intended;

(d) the right to lodge a complaint to a supervisory authority.

2. The controller shall provide the information referred to in paragraph 1:

(a) within a reasonable period after obtaining the data, having regard to the specific circumstances in which the data are processed, or

(b) if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed. [222] [223]

[221] CH suggested the same solution as in Article 14 of the GDPR to namely to replace "and, if possible …officer" with the following: " the controller may also include the contact details of the data protection officer if any**;**"

[222] DE wanted to delete paragraph 2 since it would unreasonably interfere with the work of the responsible authorities.

[223] CH suggested to complement Article 11b with a new paragraph, as in Article 14a of GDPR as follows: "3. Member States may provide that paragraphs 1 and 2 shall not apply where and insofar as:
(a) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject, which provides appropriate measures to protect the data subjects legitimate interests,
(b) the provision of such information proves impossible or would involve a disproportionate effort."

Article 11b

Limitations to the rights of information[224]

1. Member States may adopt legislative measures delaying, restricting or omitting[225] *the provision of the information to the data subject pursuant to Article 11 and 11a to the extent that, and as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned:*

(a) to avoid obstructing official or legal inquiries, investigations or procedures;

(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for[226] *the execution of criminal penalties*[227]*;*

(c) to protect public security;

(d) to protect national security;[228]

224 DE said that if Articles 11 and 11a were formulated with "may" Article 11b would not be necessary, if this was not the case Article 11b was needed. HR noted that Article 11b left broad discretion to prescribe delay, limitation or denial of this right. IT meant that there was space for improving the text in Article11b. CZ wanted to add situations to the Article, *e.g.* situations referred to in Article 14a.4 in GDPR.

225 IE suggested to replace *omitted* with *excluded* or *dispensed with.*

226 BE suggested to delete *or for*.

227 BE suggested to add: "or the prevention of danger;" so as to cover all activities of the police.

228 EE queried whether this broadened the scope of the Directive.

(e) to protect the rights and freedoms of others.

229

2. Member States may determine categories of data processing[230] which may wholly or partly fall under the exemptions of paragraph 1.[231]

232

---

229 DE suggested to insert an additional paragraph 1a containing general grounds for limiting the rights of information as follows: "1a. Member States may provide that the provision of information may be dispensed with temporarily, wholly or partly**.**
(a) if the data subject is already in possession of the information or voluntarily waives the right to the information;
(b) if the personal data are not collected from the data subject, the processing is explicitly subject to statutory regulations and the controller makes a general representation of the information referred to in paragraph 1 generally available in writing and electronically; this exception shall not apply to the collection of data in secret from the data subject;
(c) if further personal data would first have to be collected in order to provide the information;2
(d) if the effort involved in weighing the interests of the data subject in receiving the information and that required in providing the information would be disproportionate;3
(e) if this is obviously not appropriate due to special circumstances or would significantly endanger or interfere with the performance of law enforcement tasks."
IE suggested adding two new exemptions: " to protect the well-being and safety of others, in particular children. The purpose of this exemption is to ensure that the police can refuse to provide information in relation to recipients/categories of recipients of personal data where they consider it necessary to provide information to health professionals/authorities or social workers in child welfare cases; and where the provision of such information proves impossible or would involve a disproportionate effort (based on Article 14a.4(b) of the Regulation).

230 DE asked what *categories of data processing* was.

231 IT meant that it could be useful to insert that such exemptions should be set out by law.

232 CH suggested to complete Article 11b with the same wording as in Article16(2) DPFD: "3. When personal data have been transmitted or made available between Member States, each Member State may, in accordance with the provisions of its national law referred to in paragraph 1, ask that the other Member State does not inform the data subject. In such case the latter Member State shall not inform the data subject without the prior consent of the other Member State."

Article 12

Right of access for the data subject [233]

1. Subject to Article 13, Member States shall[234] provide for the right of the data subject to obtain from the controller at reasonable intervals[235] and free of charge[236] confirmation as to whether or not personal

[233] DE, ES, SI scrutiny reservation. EL wanted to limit the scope of Article 12. UK wanted to see clarifications as to whether judges' notes would be covered by the right of access. In reply to UK, the Cion said that judges' notes could be covered by Article17. SE thought that both Article 11 and 12 contained many new inflexible details and preferred the DPFD. DK found that Article 12, as well as Articles 11, 11a and 11b entailed a considerable burden on controllers. DE said that the scope was considerably different to Article 17 in DPFD and asked the reasons for this extension. LU wanted to keep the flexibility for the different national systems. The purpose could not be to harmonise national systems for criminal procedure. HR meant that the right of access should be limited to the right of notification of whether personal data of a specific person was processed by the authority and for what purpose. HR also said that the information should be provided at the request of the person concerned. DE, supported by PT, SK and UK, considered that the real issue was the scope of access, whether it was to electronic files or to paper files. Cion replied that according to Article 2.2 paper files were covered if they formed part of a filing system and that paper files constituted a filing system, see also the definition in Article 3.5. According to Cion the Charter did not make a difference between paper and processing by automated means. DE meant that the scope of the obligation would be considerable if paper files were included in the scope; the number of pages to go through. FR suggested that current Article 11 become Article 12 with the following wording: "Article 12
Information to the data subject
1. Where, within the framework of the provisions of Article 11(2), the controller proceeds to inform the data subject, the controller may provide the data subject with the following information:
(a) the identity and the contact details of the controller;
(b) the purposes of the processing for which the personal data are intended;
(c) the period for which the personal data will be stored;
(d) the existence of the right to request from the controller access to and rectification, erasure or restriction of processing of the personal data concerning the data subject;
(e) the right to lodge a complaint to the supervisory authority referred to in Article 39 and its contact details;
(f) the recipients or categories of recipients of the personal data, including in third countries or international organisations;
(g) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are processed.
(h) the possible consequences of refusing to provide the requested personal data.
2. Where Article 11(2) is applied, the controller shall provide the information listed in paragraph 1:
(a) at the time when the personal data are obtained from the data subject, or
(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection having regard to the specific circumstances in which the data are processed.
3. Where the personal data have been transmitted or made available between Member States, the Member State which transmitted the data may ask the recipient Member state not to inform the data subject."

data relating to him or her are being processed[237], and where such personal data are being processed to obtain access to such data and the following information: [238]

(a) the purposes of the processing;[239]

(b) (…)[240]

(c) the recipients or categories of recipients to whom the personal data have been or will be[241] disclosed, in particular the recipients in third countries;

---

234 CZ reservation on Member States being obliged to provide the right to access and that access be gratuitous for the data subject.

235 HU asked for a clarification of "reasonable intervals" and suggested to either add "defined by MS's law" or deleting "at reasonable intervals and free of charge" and adding a new paragraph (1a) in Article 12 with the following wording: "(1a) The information described in Paragraph (1) shall be provided free of charge for any category of data once a year."

236 UK suggested to insert the following text, along the lines with text in the GDPR, on charges: "On request and without an excessive charge, the controller shall provide a copy of the personal data undergoing processing to the data subject." IE suggested that Member States should be allowed to provide for the imposition of a small fee under paragraph 1, in particular where copies of the personal data are provided to the data subject. The Chair concluded that the question of charging a fee would be reconsidered.

237 DE preferred to set full stop after "processing". The following sentence would read: "Where such personal data are being processed, the controller shall provide the following information:"

238 ES thought that the independence of the judiciary was at stake. Support from AT, DK and UK. FI wanted to add that the right to obtain information depended on a request from the data subject made within a certain timeframe, like in DPFD. The Chair draw the attention of delegations to Article 44.2 on the relationship between the supervisory authority and the judiciary. DK noticed that the right of access had been extended compared to DPFD and that the proposal increased the burden on the police, also financially. DK considered that the same problems that it had commented on in Article 11 were present here. HU, NO, UK supported DK concerning the burden and that the problems were similar to the ones in Article 11. UK considered that Article 17.1 in DPFD was more acceptable.

239 CZ wanted to delete paragraph (a).

240 FI meant that paragraph (b) should be reinserted.

241 DE preferred to delete "or will be" since it was impossible to predict what transmission will take place in the future."

(d) (…) the envisaged period for which the personal data will be stored or the rules applicable to calculating this period [242];

(e) the existence of the right to request from the controller rectification, erasure or restriction of processing[243] of personal data concerning the data subject; [244]

(f) the right to lodge a complaint to a supervisory authority[245] (…);

(g) (…)[246]

1a. [247]Member States shall provide that where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 35 relating to the transfer.[248]

242 DE and SE welcomed the new text. UK meant that rules should precede *applicable*. Cion could accept the new text.

243 DE preferred the term "blocking" instead of "restriction of processing".

244 LU thought that paragraph 1 (e) was not a specific right but only a modality. Cion explained that paragraphs 13.1 (a)(b) and (e) intended to help MS to protect informers.

245 BE noticed that the text did not distinguish between the three categories of processing: made by the police *before* or *during* an investigation and made by the members of the judicial authority. Since the national DPA had not powers on the judicial information BE suggested to add "a judicial authority or to a court (and the contact details of the supervisory authority);" in the end of paragraph (f).

246 DE wanted to reinsert the beginning of the Cion text on paragraph (g): "communication of the personal data undergoing processing;" because it makes it easier to manage the content of data subjects' rights of access. Cion reservation on the deletion of paragraph (g).

247 FI suggested to add "Subject to/Without prejudice to Article 13" in the beginning of paragraph (1a). DE wanted to remove paragraph 1a.

248 CZ, DE and BE wanted to delete paragraph 1a; BE considered it too burdensome and that there already existed rules on this. RO wanted to move paragraph (1a) to Article 11. DE found paragraph 1a vey bureaucratic and wanted to delete it. ES feared that the provision could compromise police investigations. CZ saw the paragraph as redundant. FR in contrast had no objections in principle against the paragraph. Cion said that the paragraph was not a new element; it already existed in GDPR (Article 15.1a) and should stay in the text.

2. (…)[249]

2. Profiling shall not be based on special categories of personal data referred to in Article 8(1), unless Article 8(2) applies and appropriate safeguards for the rights and freedoms of the data subjects are in place. [250]

Article 13

Limitations to the right of access[251]

[249] Cion reservation against deletion because this goes beyond what is set out in DPFD.

[250] DE wanted to delete the redrafted paragraph 2 since it did not add anything more than Article 8, supported by IT for the reason that Article 20.2 in the GDPR has been deleted.

[251] ~~BE~~, DE. BE reservation in substance. BE explained that in BE limitations are not on a case by case basis but are set out as total legal exceptions. FR wished to introduce the possibility of an indirect access and noted that DPFD did not forbid indirect access. DK mentioned that Article 52 in the Charter sets out the limitations and deemed it important that the limitations did not become the rule. ES and HU argued that Article 13 did not solve its problem concerning the independency of the judiciary that ES had mentioned in relation to Article 12. BE supported the FR text in DS 1850/12. SE wanted criminal intelligence to be listed in paragraph 1 allowing to restrict the data subject's access. UK joined SE and required more flexibility allowing for tailoring of the national systems. For UK Article 13 should only contain minimum standards. CZ was of the opinion that the scope of Article 13 depended on the particular situation in a particular state. NL considered that it should be possible to deny access on behalf of the MS that provided the information. DE thought that other exceptions could be added to the list. UK was broadly in agreement with the Article.Cion said that restrictions should be allowed only when it was really necessary and that the principle was direct access; indirect access could be acceptable if needed. FR suggested to move Article 13 to become Article 10 with the drafting set out in the footnote. FR further suggested that current Article 12 become Article 13 with the following wording: "*Article 13*
Right of access for the data subject

1. *Member States shall provide for the right of the data subject to exercise his or her right of access by contacting the supervisory authority. Upon conclusion of the access procedure and any rectifications under Article 15, the supervisory authority shall inform the data subject that it has carried out the necessary verifications.*
2. *Member States may provide that the right of access to data is exercised through direct contact with the controller, where this does not prejudice the purposes of the data processing.*
3. *Member States may provide that the following information are transmitted to the data subject, where this does not prejudice the purposes of the data processing:*

(a) *the purposes of the processing;*
(b) *the categories of personal data concerned;*
(c) *the recipients or categories of recipients to whom the personal data have been disclosed, in particular the recipients in third countries;*
(d) *the period for which the personal data will be stored;*
(e) *the existence of the right to request from the controller rectification, erasure or restriction of processing of personal data concerning the data subject;*
(f) *the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;*

1. Member States may adopt legislative measures[252] restricting[253], wholly or partly, the data subject's right of access to the extent that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned:[254]

(a) to avoid obstructing official or legal inquiries, investigations or procedures;

(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties[255];

(c) to protect public security;

(d) to protect national security; [256]

(e) to protect the rights and freedoms of others. [257]

2. Member States may determine by law categories of data processing[258] which may wholly or partly fall under the exemptions of paragraph 1.[259]

(g) communication of the personal data undergoing processing and of any available information as to their source.

4. Member States shall provide for the right of the data subject to obtain from the controller a copy of the personal data undergoing processing.

5. Member States shall provide that the controller informs the data subject of the possibility of seeking a judicial remedy."

252 HR meant that it should be set out in law and not in legislative measures.

253 CH suggested to add "delaying" after "restricting".

254 CZ asked to add another subparagraph to paragraph 1 relating to children involved in household violence.

255 BE wanted to add "and the prevention of danger;"

256 FI asked that the changes to the draft Regulation on restrictions (Article 21) be mirrored here.

257 FI suggested reverting to the text in Article 17.2(e) in the DPFD. CZ wanted to add "and of the data subject" in the end of the paragraph to cover cases of domestic violence for example Cion wanted that this paragraph be aligned to Article 21.1(f) of GDPR.

258 DE considered that it was still unclear what was meant with "categories of data processing".

259 NL preferred deleting paragraph 2 since it considered that the grounds for refusal were sufficient.

3. In cases referred to in paragraphs 1 and 2, Member States shall provide that the controller informs the data subject (…) of any refusal or restriction of access, of the reasons for the refusal [260] or the restriction[261] and of the possibilities of lodging a complaint to the supervisory authority[262] and seeking a judicial remedy[263]. This shall not apply (…) where the provision of such information would undermine a purpose under paragraph 1. [264]

4. Member States shall ensure that [265]the controller documents the grounds for omitting the communication of the[266] factual or legal reasons on which the decision is based. [267]

---

260 FI suggested to insert "or restriction" after "refusal".

261 ES, HU and CZ supported the addition to the text.

262 AT meant that it would be useful for the data subject to know to what SA he or she should lodge a complaint, this might also be done in a recital.

263 NL wanted to remove the brackets because it should always be possible to seek a judicial remedy.

264 DE, CH and CZ saw problems with this paragraph because the data subject can draw conclusions on the basis of a motivated refusal. UK meant that it is implicit in paragraph 3 that the reply is negative. In the UK the reply can be "neither confirm nor deny" since a negative reply also contains information. Cion stressed that this paragraph did not interfere with the MS national criminal procedures. DE suggested to delete paragraph 3 because of the changes it has suggested for Article 10.4a. AT suggested a new drafting for paragraph 3 as follows: "3. In cases referred to in paragraphs 1 and 2,or when, in fact, no data on the person requesting the information is processed, Member States shall provide a neutral reply, instead of giving a reason in substance, stating that "no data are being used which are subject to the right to information". In addition, an information on the possibilities of lodging a complaint to the supervisory authority **or, where applicable the seeking of a** judicial remedy shall be given." BE said that in BE the data subject must address him-or herself to the supervisory authority to have access to information and that the data subject is not informed about refusal/restriction of access. ES pointed out that Article 10.4 would need to be redrafted if the provision in paragraph 3 was maintained.

265 DE suggested to insert "in cases of Article 10(3)(2) between that and the controller.

266 IE suggested to replace " for omitting the communication of the" with " for not communicating the …'.

267 CZ saw other problems here since the information that personal data was being processed can be useful. CZ considered that the paragraph was redundant because of Article 18. CZ meant that the paragraph was not fully harmonised with the last sentence of paragraph 3. UK considered that this paragraph was superfluous. BE feared that the Article could lead to the harmonisation of the criminal procedure. BE said that since there is not direct access in BE the controller did not keep documents.

Article 14

Additional modalities for exercising the right of access[268] 269

1. Member States shall provide for the right of the data subject to request, in cases referred to in Article 13[270], that the supervisory authority checks the lawfulness of the processing. [271]

2. Member State shall provide that the controller informs the data subject of the right to request the intervention of the supervisory authority pursuant to paragraph 1. [272]

---

[268] BE and FR reservation in substance. FR, UK scrutiny reservation. UK raised concerns that it may lead to a controller being obliged to send the DPA very sensitive data which could prejudice investigations. UK thought that a clause similar to the one in Article 13.3 would be the appropriate solution. DE, RO and SI found this Article was redundant; DE pointed to Article 45.1 (b) and 45.2 and RO pointed to Article 12.1(f) that already covered Article 14.2; DE wanted to delete Article 14 and SI would not oppose it if other delgations wanted it. FR expressed doubts about the utility of the Article. SE meant that Article 14 set out selfevident elements and contained too many details but could accept the Article if the SA could decide him or herself what measures should be taken. Cion meant that Article 14 was an important provision and wanted to keep it and reintroduce paragraph 3 that had been deleted.

[269] RO considered that the title of the Article should be changed to "Right to lodge a complaint to the national supervisory authority". Support from FI, AT and SE. UK whished to know whether this Article was needed since Article 50.1 provided for this obligation. FR wanted to delete current Article 14 since its content was inserted in Article 12 as suggested by FR. FR considered that Article 15 and 16 could be merged and become Article with the following wording: "*Article 14*
Right to rectification and erasure

1. *Member States shall provide for the right of the data subject to obtain from the controller the rectification or erasure of personal data relating to them which are inaccurate or which do not comply with Articles 4, 7 and 8 of this Directive. The data subject shall have the right to obtain completion of incomplete personal data, in particular by way of a corrective statement.*
2. *The controller shall carry out the rectification or erasure without delay.*
3. *Member States shall provide that the controller informs the data subject in writing of any refusal of erasure of the processed data and the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy."*

[270] BE suggested to add references to Articles 11b and 15.

[271] PT wanted to know if paragraph 1 allowed for a direct or indirect access. BE, ES and IT likewise. DE wanted to delete paragraph 1 because the content is already covered in Article 45 (1)(b). BE wanted to remove paragraph 1. BE meant that the MS could organise an indirect access via the DPA who would inform the data subject that a control has been carried out.

[272] RO did not see the differences between Article 12.1 (f) and paragraph 2 of this Article. DE suggested to delete paragraph 2 since the content is covered by Article 10(3) in its wording suggested by DE.

3. **When the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications by the supervisory authority have taken place, and of the result as regards the lawfulness of the processing in question**.[273]

Article 15

Right to rectification, erasure and restriction of processing [274]

1. [275]Having regard to the nature and purpose of the processing concerned, Member States shall provide for the right of the data subject to obtain from the controller the rectification of personal

[273] At the request of FI paragraph 3 was reinserted.

[274] DE, ES, PT and SI scrutiny reservation. EE reservation. DE considered that the Article increased the administrative burden. CZ, SI and FR preferred the text of Article 18 in DPFD. AT wanted to know the purpose with the Article. UK wanted to see recital 21 be incorporated in the body of the text. EE thought that the Article was too far reaching and that it was necessary to set out the type of data that could be rectified as well as the reasons and justifications for the request to rectify. UK meant that only facts and not personal assessments could be rectified. DE considered that the overall relationship between Articles 4(d), 15(1) and 15(1a) was unclear. DE queried why Article 15 differed from Article 18 of DPFD. DE meant that the accuracy or inaccuracy of statements could not be determined at the level of data protection law but is the main purpose of investigations and the criminal proceedings. DE thought that what the Directive should set out was mere blocking and not the obligation to erase. HR suggested that rights set out in the Article only be carried out *ex officio*, otherwise the effectiveness of the criminal proceedings could be compromised. CH preferred the term "blocking" instead of "restriction". SE wanted to see *blocking* as well to take into consideration legislation on archives which have requirements on keeping information. FI suggested to include the same text as in Article 4.4 of DPFD. FR meant that flexibility should be given to authorities regarding the purposes pursued. BE said that Article 15 did not correspond to the BE system where it was the DPA that asks for rectification, erasure and restrictions of processing. SE meant that restriction was more of a temporary measure than blocking which exists in DPFD and that SE did not approve of the change of terminology. SE further said that it is forbidden in the SE Constitution to erase personal data. UK meant that recital 15 was helpful and that the text therefore could be added to the Article. FR wanted to insert a reference to indirect access in the different paragraphs. DE asked when data should be erased respectively restricted and meant that authorities should not erase only because a time limit had expired, also because it was difficult to erase retained data; it should be enough to block the data. DE pursued that it was very expensive for authorities to erase data it should be enough to block/restrict data and this had to be set out in the Directive. For DE it was very important that the Directive did not require 100 % erasure.

[275] BE suggested to add a new Article 15a on the limitations on the rights to rectification, erasure and restriction of processing and in line with that suggestion it wanted to add “Subject to Article 15a ...” in the beginning of each paragraph of Article 15. IE supported the BE suggestion on the addition of an Article15a.

data relating to him or her [276]which are inaccurate[277] and (…) the right to obtain completion of incomplete personal data, including by means of providing a supplementary statement. [278]

[276] HR suggested to insert "in any way (inaccurate, left and false, incomplete, inaccurate, outdated etc)".

[277] FI and UK were concerned about witness testimonies. DE, supported by SE, saw the problem of rectification as a problem of substance rather than of data protection. SE thought that rectification only concerned "dry rectification of obvious facts" and wanted to clarify the Article with this in mind. DE found it important that data that were inaccurate could be corrected.UK voiced concerns over *who* defined "inaccurate" and asked what type of data could be rectified. Cion thought about how to link *inaccurate* in Article 15 and Article 4.1(d) if it gave reason to erasure or how to frame it. DE noted that erasure did not exist in Article 4 and that it wanted a balance between the rights and obligations (of the data subject and the controller).

[278] SE, CZ, NL, AT and RO did not understand the end of the sentence of paragraph 1 and RO considered that the paragraph had not added value. Cion reservation. DE suggested to replace the underlined text with the following: " if the addition is relevant for the purposes referred to in Article 1(1)." DE meant that the addition prevented misuse. AT suggested to delete the underlined text. Cion informed that *supplementary statement* had the same meaning as in the GDPR and that a rectification of the initial text was not possible in all cases but that it could be set out in the statement and the purpose was not to limit for the MS how to rectify. FR asked that the Cion explanation of the supplementary statement should be set out in a recital. Cion confirmed DE that the purpose was not to rectify what the data subject had said. Cion set out that the assessment of the accuracy was to be based on objective criteria.

1a. [279]*Member States shall provide for the obligation of the controller to erase personal data*[280] *without undue delay and of the right of the data subject to obtain from the controller the erasure of personal data (…) without undue delay where the processing does not comply with the provisions adopted pursuant to Articles 4 (a) to (e)*[281]*, 7 and 8 of this Directive*[282]*, or where the data have to be erased for compliance with a legal obligation to which the controller is subject.*[283]

1b. [284]Member States shall provide for the right of the data subject to obtain from the controller the restriction of the processing of personal data where their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data, or where they are required by the data subject for the establishment, exercise or defence of legal claims.[285]

[286]

---

279 BE wanted to add "Subject to Article 15a ..." in the beginning of each paragraph of Article 15.

280 CH suggested to replace the text between "without undue delay …without undue delay" with the following text: of the data subject of its own motion or upon request and without undue delay where".

281 HU noted that the figure "1" after "4" and Cion agreed to this.

282 ES meant that the reference to Articles 4 (a)-(e), 7 and 8 was too broad.

283 DE suggested to delete the paragraph because it meant that the obligation to erase should be dealt with separately in Article 16, as in the Cion proposal. ES wanted to put the paragraph in square brackets because it considered that not any irregularity should necessary lead to the erasing of data. UK strongly pushed for a derogation to retain personal data when the controller is subject to a legal obligation. UK found that the exceptions were not clearly set out. Cion said that paragraph 1a went back to now deleted Article 16.

284 BE wanted to add "Subject to Article 15a ..." in the beginning of each paragraph of Article 15.

285 DE suggested to delete paragraph 1b because data whose accuracy was contested by the data subject could not be blocked in criminal proceedings or proceedings for the purpose of threat prevention. CH suggested to reword paragraph in the following way: "1b. Member States shall provide for the right of the data subject to obtain from the controller the **blocking of the processing of personal data where their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the dat**a." NL meant that this was a far-reaching provision. UK found that the exceptions were not set out clearly.

286 CH wanted to add the following paragraph: "1bb. Member States may/shall provide that in case where the accuracy of an item of personal data is contested by the data subject and its accuracy or inaccuracy cannot be ascertained, referencing of that item of data may take place. Personal data shall be blocked instead of erased if they are required by the data subject for the establishment, exercise or defense or legal claims." CH explained that the addition of paragraph (1bb) was necessary in order to make sure that activities of public authorities should not be jeopardized in any way.

2. [287]Member States shall provide that the controller informs[288] the data subject (…) of any refusal of rectification, erasure or restriction of the processing, the reasons for the refusal and the possibilities of lodging a complaint to the supervisory authority[289] and seeking a judicial remedy. [290]

3. [291]Member States shall provide that in the cases referred to in paragraphs 1, 1a and 1b[292] the controller shall notify the recipients and that the recipients shall rectify, erase or restrict[293] the processing of the personal data under their responsibility.[294]

---

287 BE wanted to add “Subject to Article 15a ...” in the beginning of each paragraph of Article 15.

288 UK believed that the controller’s ability to refuse the request was not sufficiently set out and would prefer text similar to prefer text similar to Article 13.1 and a clear stipulation that the controller may refuse if complying would prejudice the prevention, detection, investigation, or prosecution of crime or in negatively impact public security in other ways. In order to limit the obligation to communicate the refusal UK suggested inserting the following text: “This shall not apply where the provision of such information would undermine a purpose under Article 1". For UK a "neither confirm nor deny" provision vital. FR supported the UK and found the obligation to systematically motivate a refusal went too far.

289 SE wanted to insert "court" after "supervisory authority".

290 UK thought that it was not always appropriate to indicate why a rectification had been carried out and feared that it could jeopardize an ongoing investigation. DE suggested to delete paragraph 2 because its content is covered by Article 10(3). CH also wanted to delete paragraph 2. NL wanted to remove the square brackets.

291 BE wanted to add “Subject to Article 15a ...” in the beginning of each paragraph of Article 15.

292 Since DE wanted to delete paragraphs 1a and 1b DE suggested to delete the reference to those paragraphs. CH suggested to add its new paragraph (1bb).

293 DE wanted to delete "erase and restrict".

294 DE wanted to add the following text to the end of the sentence: " if these measures are important for the recipient or necessary to protect the data subject's rights." DE scrutiny reservation. DE meant that despite its addition it was necessary to decide whether the the provision should be further lifted. DE said that the broad legal definition of recipients could create problems for the application of Article 15(3). Cion wanted to think about how to frame paragraph 3.

295

Article 16
Right to erasure

(…)[296]

---

295 BE suggested, supported by IE, a new Article 15a as follows: *"Article 15a* **Limitations to the right to rectification, erasure and restriction of processing**

1. Member States may adopt legislative measures delaying, restricting or omitting the right to rectification, erasure and restriction of processing of the data subject pursuant to Article 15 to the extent that, and as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the individual concerned:
   (a) to avoid obstructing official or legal inquiries, investigations or procedures;
   (b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences, the execution of criminal penalties or the prevention of danger;
   (c) to protect public security;
   (d) to protect national security;
   (e) to protect the rights and freedoms of others.
2. Member States may determine categories of data processing which may wholly or partly fall under the exemptions of paragraph 1.

296 DE suggested to insert the following text in Article 16: "1.Member States shall provide for the right of the data subject to obtain from the controller the erasure of personal data relating to them without undue delay where the processing does not comply with the provisions adopted pursuant to Articles 4 (a) to (c) as well as 7 and 8 of this Directive. The same applies if the processing does not comply with the provisions adopted pursuant to Articles 4 (e); in these cases the controller may anonymise the personal data instead of erasing the.

2. Instead of erasure, the controller shall block the personal data where the conditions under Article 4a (3) are met."

DE meant that paragraph 2 corresponded to the rights of the data subject and would lead to harmony with Article 4(3)(a). For DE the obligation to erase means that data at least in files do not have to be erased as long as doing so would violate the principle enshrined in the DE Constituion that files must be complete and accurate.

Article 17

Rights of the data subject in criminal investigations and proceedings[297]

Member States may provide that the exercise of the rights (…) referred to in Articles 11, 11a, 12 and 15[298] is carried out in accordance with national procedural law[299] where the personal data are contained in a judicial[300] decision or record[301] or case file processed in the course of criminal investigations and proceedings. [302]

---

297 BE and IE reservation of substance on the application of the Article on courts and tribunals. SE asked for an analysis of the application to courts and tribunals. BE meant that the Directive could be applicable to data banks but that its application to pre- trial investigation was doubtful; the discussion on Article 15 also showed that. In contrast CZ and SE welcomed the changes, CZ meant that the Article could also be removed. PT found Article 17 superfluous. Cion said that Directive 95 applies to civil courts but not to criminal proceedings. BE contested that Directive 95 was applicable to courts and tribunals and meant that the judicial code put in place a system of an equitable process and that it would not be that easy to mix data protection and data protection in a single code. SE and SK supported BE fears about the mixing of criminal procedure law and data protection. SE meant that reference could be made to Article 14 as well. DE feared a creeping harmonisation of the criminal procedure law. DE referred to a statement by the Commission which lead to the conclusion that Article 17 must be interpreted as a purely declaratory provision, DE therefore required that Article 17 be clarified. FI considered it impossible to comment on the Article since it was not clear what was intended and suggested to either delete or redraft the Article. SE considered that the Article clashed with national criminal procedure law and that the exceptions set out were not sufficiently broad. SE said that courts had information that did not form part of the judgement or the minutes of the process. SI asked about the differences between Article 4.4 in DPFD and Article 17 and meant that Article 17 was more "dangerous" since the scope of the Directive also covered domestic processing. FR supported the Article.

298 DE suggested to add "Article 16". Cion considered that a reference to Article 14 could be added.

299 CH suggested to replace the paragraph from "where the personal data" until the end of the sentence with the following: " where the personal data are processed in the course of criminal investigations and proceedings.". IE reservation of substance on the insertion of *procedural law* whereas DE welcomed it. IE meant that *national procedural law* narrows the scope. ES scrutiny reservation on the notion *national procedural law*. SK found that *national procedural law* would create problems for criminal law. SI meant that *national procedural law* could be dealt with in the recitals.

300 HU suggested to add "police and public prosecutorial" after *judicial decision* and DE asked if prosecutors' *decisions were covered as well.* HR supported the addition of *police* after decision.

301 BE asked when a police record becomes a judicial record and thought that it was necessary to define "judicial". HU wanted to add "documents, registry and decisions of police and public prosecutors". UK and IE asked clarification on the meaning of judicial decisions and records. EE thought that more flexibility should be considered.

302 AT, BE, SI and PL queried the need of the Article if the purpose was, according to the Cion, only to set out modalities. On the opposite, NO considered the Article necessary and that it should be applicable to both the police and the judiciary. DE shared NO view and commented that Article 4.4 in the DPFD contained a similar provision. CZ, NL, SE preferred the wording of the DPFD. SE thought that the scope had become broader than in the DPFD. EE considered that the Article had become more ambiguous and wanted it to be clearer. HU wanted to cover decisions by the police, the public prosecutor and criminal proceedings. ES also wanted to include police proceedings as it

CHAPTER IV

CONTROLLER AND PROCESSOR[303]

SECTION 1

GENERAL OBLIGATIONS

Article 18

Obligations of the controller [304]

1. Member States shall provide that the controller implements appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance[305] with the provisions adopted pursuant to this Directive.

1a. Where proportionate in relation to the processing activities[306], the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies[307] by the controller [308] which specify the application of the data protection rules adopted pursuant to this Directive.[309]

---

was not always easy to know when one kind of proceedings finished and another started. It suggested to reword the text "rights set out in the Directive" or to let the MS decide how to protect fundamental rights. DE supported this view. FI meant that at least the words "and proceedings" should be deleted.

303 PT scutiny reservation on Chapter IV.

304 UK considered that Article 18 was superfluous since it duplicates Article 4(f). ES considered the Article purely rhetoric. IT scrutiny reservation on Article 18. FR found it important to address the delimitation of competencies between the controller and the processor. FR meant that it was necessary to make sure that the rules in GDPR and this instrument were compatible and consistent.

305 DE meant that it remained unclear which specific conditions the new obligation to demonstrate compliance could, may and must meet. In particular, it was not clear how this obligation related to the documentation and logging obligations in articles 23 and 24.

306 RO thought that the words *proportionate in relation to the processing activities* were too vague and did not leave room to ensure conformity with the stipulations of the Directive.

307 In view of Article 19, RO asked for a clarification of the term *policies*, DE too and what significance it had for *measures* referred to in paragraph 1 and 1a. CZ, supported by FR, also asked for clarifications on what was meant with *policies* CZ considered it superfluous and that it therefore should be deleted.

308 FR scrutiny reservation.

309 DE suggested to remove the last part of paragraph 1a as well as in recital 38.

2. (…)[310]

Article 19[311]

Data protection by design[312] ***and by default*** [313]

1. [314]Member States shall provide that, having regard to available technology[315] and the cost of implementation and taking account of the risks for rights and freedoms of individuals posed by the nature, scope and purpose of the processing, the controller shall implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of provisions adopted pursuant to this Directive[316] and protect the rights of the data subject.

2. Member States shall provide that the [317] controller shall implement [318]mechanisms[319] for ensuring that, by default, only those personal data which are necessary[320] for the purposes of the processing are processed. [321]

---

310 DE wanted to restore paragraph 2 in the Cion proposal, since it helped specify the term *measures.* Cion had no problems with such reinsertion.

311 DE and RO scrutiny reservation on Article 19. Cion explained that the reasons to maintain the Article were the same as in the GDPR and that the principles were necessary, that they applied to all stages in the processing and not only to automated processing. DE wanted to add after *MS shall provide ... in* both paragraphs the following text: "in automated processing ..."

312 FR meant that since the concept of *privacy by design* was incompatible with the data processing existing at the entry into force of the Directive it would be necessary to insert a provision indicating that the existing processing operations created and implemented in accordance with the legislation in force before the entry of this proposal would be maintained.

313 FR reservation. UK, supported by RO, supported the principle in Article 19 and considered that the text must be flexible and considered that the text would be better placed in the recitals. UK further considered that the purpose should not be to set out "the state of the art" because it could be expensive. SE also supported the principle. SE did not consider it appropriate to legislate directly but that such principles should be set out in a recital. SI expressed doubts about the whole Article 19 and suggested to delete it since it was not appropriate for police and judicial cooperation. SI scrutiny reservation. EE asked about the aim of the Article. EE generally supported the idea of data protection by design and by default. DE also wanted to see a more flexible text. With a reference to Article 2.2 and recital 15, DE considered that the Directive covered this all way. DE suggested to set out in Article 19 what can be achieved "insofar as possible", since this would make the Article more flexible. NO thought that the Article was unclear and that the links to other Articles were unclear.

314 DE suggested adding "In automated processing systems" before *Member States.*

315 FR scrutiny reservation on the term "available technology".

316 FR wanted to delete the words "meet the requirements … this Directive" because FR did not find it necessary.

317 DE suggested adding "In automated processing systems" before *the controller.*

Article 20

Joint controllers [322]

Member States shall provide that where a controller determines the purposes (…) and means of the processing of personal data jointly with others, the joint controllers must determine the respective responsibilities for compliance with the provisions adopted pursuant to this Directive, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them[323], unless the respective responsibilities of the controllers are determined by Union[324] or Member State law to which the controllers are subject. [325]

---

318 DE suggested adding "as far as is feasible and appropriate" before *mechanisms.*

319 DE meant that it was unclear what was meant by *mechanisms.*

320 ES suggested to replace *necessary* with *appropriate* to provide more flexibility and said that the wording of Article 4.1 (c) was better. Cion said that necessary related to the minimisation principle. Cion further said that the proportionality of cost was the guidance and that cost could also be set out in paragraph 2.

321 ES wanted to entirely revise paragraph 2 and considered that what was set out was not a minimisation. AT asked about the general obligation in paragraph 2 and how it was evaluated. DE, SE and CZ considered that proportionality should be addressed in paragraph 2 as well. CZ suggested to add a reference to "the state of the art and the cost" in paragraph 2 too. FR and CZ wanted to delete paragraph 2 since it was redundant.

322 ~~EE and~~ DE scrutiny reservation. FR declared that they were opposed to this notion.

323 FR asked that the text "by means of agreement … between them" be deleted because the legislator should not set out by what means the national legislator implements the Directive. CH meant that the first reference should be to law since the controller was likely to be a public body.

324 FR had problems with the reference to Union law.

325 SI suggested to add "by national law" if the controllers were two public authorities. Support from DE, CH, CZ, FR, IT, LV, PL, PT, RO, SE. ES considered that the text lacked information about to whom the data subject could turn to exercise his/her rights. PL also thought that it was important to know which one of the controllers was responsible.

Article 21

Processor[326]

1. Member States shall provide that the controller shall use only (…) processors providing sufficient guarantees to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of the provisions adopted pursuant to this Directive (…).[327].

2. Member States shall provide that the carrying out of processing by a processor shall[328] be governed by a legal[329] act[330] binding the processor to the controller and stipulating in particular [331]that the processor shall act only on instructions[332] from the controller (…).[333]

3. (…)

---

326 UK thought that Article 21 was crucial and that the role of the processor and controller had to be discussed. PL asked if the processor could only be a public authority and BE wanted to know what would happen if the processor was not a public authority. Cion indicted that Article 17 and 22 in DPFD set out the same obligations. FR stated that they wanted that the processor's responsibilities be clarified and specified in a summary Article. On Articles 21 and 22 and as in GDPR, BE said that controllers may need to use consulting companies for the processing and that they may not now who is processing their own data, for the sake of legal certainty the Directive should regulate the relation between all controllers and processors in judicial and police matters taking into account the Decision of the Cion on international transfer.

327 FI and UK wanted to delete paragraph 1. DE scrutiny reservation, because it had not yet been decided whether the principle of Article 21 (1) should be extended to cases in which IT systems are maintained by external firms.

328 DE wanted to replace *shall* with *must.*

329 CH suggested to add "or contractual" because they thought that legal act was too narrow.

330 UK queried the precise meaning of *legal act* and sought clarification about whether a contract was sufficient. IE suggested to replace *act* with *instrument.* DE suggested to remove *act* and add "provision or contract". DE said that if it was not clear between the MS how the competencies between the controller and processor were delimited they would interpret the whole text differently.

331 FI asked to delete the end of paragraph 2 after "in particular". Support from AT, BE, FR, SE. NO and SE wanted to know if it was necessary to set out "by a legal act" and if a contract would not be enough, such was the situation in NO. Support from CZ, DE, UK. DE found the paragraph confusing and could be deleted.

332 DE preferred to use "within the scope of" rather than "on instructions from".

333 SI scrutiny reservation.

Article 22

Processing under the authority of the controller and processor[334]

(…)

[334] Cion reservation on deletion, referring to Article 21 of DPFD.

Article 23

Records of categories[335] of personal data processing activities[336]

1. Member States shall provide that each controller and processor shall maintain a record[337] of all processing systems (…) under their responsibility.[338]

2. (…)

3. The controller and the processor shall make such records available, on request, to the supervisory authority.

---

335 UK sought clarification on what category or type of record was required by the Article, *e.g.* was it necessary to list every single type of processing or was it enough to keep categories such as *defendant data* and *witness data?* BE, supported by DE, PT and RO, asked what was meant with *categories* and noted that no explication was provided in the recitals. DE noted that this wording did not correspond to the wording in DPFD or Article 28 in GDPR and that the provision was stricter and that DE said no to these stricter rules.

336 SI and PT scrutiny reservation. CH meant that the title should correspond to the content of the provision and therefore replace "activities" with "systems". FR meant that the notion *processing* activities was too large and that it was necessary to frame it. RO asked what the data in this Article may contain and who would check whether this record was properly documented. DE noted that Article 23 and especially Article 24 derogated from the documentation obligation in Article 10 of DPFD and Article 28 of GDPR. DE further considered that the terminology in both Articles remained vague and therefore problematic. CZ suggested to copy Article 28.1 from GDPR. BE considered that the title was problematic.

337 UK asked what kind of records/categories were intended.

338 FR had concerns about the term *all processing systems* in paragraph 1 and meant that it should be defined, since it could potentially imply an extension of the obligation to maintain documentation since it may in practice prove impossible to implement this article for existing processing operations. IT meant that it would be better to replace *systems* with *operation.* CZ meant that the text in Article 28.1 of GDPR was better. BE suggested to clarify the term in a recital.

Article 24

Logging[339]

1. Member States shall [340]ensure that logs are kept of at least the following processing operations: collection, alteration, consultation[341], disclosure, [342], combination or erasure[343] in automated processing systems[344]. The logs of consultation and disclosure shall show [345](…) the purpose[346],

---

339 DE, UK scrutiny reservation. NO reservation. ES feared that the Article would cause administrative burden and suggested to remove the Article. DE considered that the obligation to keep record created un disproportional bureaucracy. PT raised concerns regarding the proportionality of the obligation and the administrative burden it would entail. FR agreed to the objective of the Article but did not want to extend it beyond the requirements of Article 10 in DPFD. Like FR, IT saw the need for having a policy on records keeping
DE noted that Article 23 and especially Article 24 derogated from the documentation obligation in Article 10 of DPFD and Article 28 of GDPR. DE further considered that the terminology in both Articles remained vague and therefore problematic. DE suggested the following new wording for Article 24: "1.In automated processing systems all transmissions of personal data shall be logged or documented for the purposes of verifying the lawfulness of the data processing, self-monitoring and proper data integrity and security. 2. Logs or documentation prepared under paragraph 1 shall be communicated on request to the competent supervisory authority to monitor data protection. The competent supervisory authority shall use this information only to monitor data protection and ensure proper data processing as well as, data integrity and data security." DE concluded that it had not yet finished its deliberations as to whether the obligation to document is to be introduced for all transmissions or only in automated processing systems. SE said that logging related to possibility to trace and security of information and that the Article therefore should be better placed after Article 27. IT meant that is was an important Article, compared with Article 10 DPFD and for Prüm. NL had doubts about the purpose and meant that the Article seemed more linked to documentation. FR meant that the Article potentially implied a heavy burden on the controller; FR therefore suggested to adapt the obligations depending on the risks and add "as far as possible" in the beginning of the sentence. UK meant that a reference to proportionality was necessary. AT asked what would happen if the data was not subject to automatically registration. PT meant that the order of the paragraphs in Article 24 could be reversed.

340 FR, ES suggested to move the words *as far as possible* to after the "The MS shall".

341 EE asked what consultation covered.

342 EE asked whether disclosure to the press was meant here.

343 UK questioned the need or appropriateness to say that data had been erased (retained) since this was disproportionate. UK suggested that a risk assessment could be made. DE thought it necessary to set out a time line for erasure.

344 UK sought clarification as to whether the logging requirement only concerned *automated processing systems.* Cion reservation on the insertion of *automated processing systems.* Cion said that Article 10 in DPFD was an important Article. DE considered that Article 10.2 in DFPD only related to automated processing and that the drafting of Article 24 created a heavy burden.

345 RO wanted to insert "at least" between *show* and *the purpose*, so that MS would have the possibility to provide for extra options to be shown in logs in order to thoroughly document the processing operation.

346 CH, EE, ES, FR, SE wanted the reference to purpose to be deleted. In contrast AT thought that it was important to keep the reference to purpose. SE said since a log never could show the purpose

date and time of such operations and, as far as possible[347], the identification of the person who consulted or disclosed[348] personal data. [349]

2. The logs shall[350] be used (...) for the purposes of verification of the lawfulness of the data processing, self-monitoring and for ensuring data integrity and data security. [351]

---

of the transaction, only that someone had done something with the data the word *purpose* should be deleted. UK wanted that a reference to proportionality should be added.

[347] FR and ES wanted the phrase *as far as possible,* to be moved to the start of paragraph 1, and that the word *purpose* to be deleted from that paragraph because this article potentially imposes very demanding obligations on controllers given the various existing types of data processing, and specifically that this obligation should be adjusted in accordance with the risks presented by the data processing. SK wanted to remove the words *as far as possible.* FR suggested the following drafting for Article 29.1: " As far as possible, Member States shall ensure that records are kept of at least the following processing operations: collection, alteration, consultation, disclosure or erasure in automated processing systems. The records of consultation and disclosure shall show in particular the date and time of such operations and the identification of the person who carried out such operations."

[348] RO asked clarifications if consultation and disclosure included the possibility that the dat**a** were consulted by other police authorities (of another State/"transfer" of data).

[349] EE ~~and CH~~ considered that the paragraph was too restrictive. UK had concerns about the purpose and practical difficulty of keeping such records, especially those of *erasure.* UK thought that such records might entail disproportionate costs and burdens and suggested a reference to proportionality and the cost involved.

[350] FR asked to replace *shall* with *may.*

[351] BE reservation of substance on paragraph 2. ES wanted to extend the scope of the Article or clarify the text. DE asked who was addressee of the obligation. Cion explained that it was, like in Article 23.3, both for internal and external use. BE wanted to add the following text to the end of paragraph 2: "and for the purposes set out in Article 1.1." because logs could be useful for operational purposes, *e.g.* two persons say that they don't know each other but the logs sow that they have been controlled in the same car.

Article 25

Cooperation with the supervisory authority[352]

(…)

Article 26

Prior consultation of the supervisory authority[353]

2. Member States shall ensure that the controller or the processor consults[354] the supervisory authority prior[355] to the processing of personal data which will form part of a new [356]filing system[357] to be created[358] where:

(a) [359]special categories of personal data referred to in Article 8 are to be processed[360];

(b) the type of processing, in particular where using new technologies, mechanisms or procedures, involves specific risks for the (…) fundamental[361] rights and freedoms (…) of data subjects. [362]

---

352 NL regretted the removal of Article 25.

353 FR considered that it was an important Article, like Article 23 in DPFD. ES said that the title and the drafting were problematic and did not see the added value of the Article. ES suggested to change the Article in line with the changes made to the Regulation. Scrutiny reservation for UK, DE, ES, SI, SE reservation.AT wished to see a follow-up to the consultation inserted in the Article. UK questioned the appropriateness for the SA to have oversight on law enforcement or public security matters which it may not have competence to judge. DE still examined whether the provision was proportionate to the benefit it provided. SI thought that Article 23 in DPFD should be used as a model for drafting. HU suggested to use the text of the GDPR (Article 34.2).

354 FR wanted to know the value of the consultation, was it a simple consultation or were legal consequences attached to it. DE said that for small files and for urgent matters it would be no time to consult.

355 ES did not see any need for prior consultation and wanted it removed as had been done in the Regulation.

356 DE suggested inserting "automated" before *filing system* because non-automated files and filing systems did not pose a threat justifying prior consultation of the SA.

357 SE and UK asked why a new filing system triggered the consultation of the SA; SE especially when a new system was created by law. UK believed that it might be overly burdensome.

358 FR would like the phrase *a new filing system to be created* to be replaced with *processing.*

359 DE suggested adding "significant quantities of" before *special categories* because a single incidence of processing individual sensitive data must not be subject to the obligation to prior consultation. DE considered that it was necessary to consider whether a limitation was appropriate for those files which were kept only a short time before being erased.

360 UK meant that if the controller had already taken appropriate precautions while processing special category data prior consultation should not be needed if they begin a new filing system, paragraph 1(a) could therefore be removed.

363

361 NL accepted the insertion of *fundamental* and wanted it inserted in recital 41 vas well. In contrast SI wanted to delete *fundamental*.

362 To UK it ~~also~~ seemed unnecessary to consult when the data systems were updated. DE wanted it to be clarified that the consultation should take place only for automated processing. UK believed there was a need for alternative wording which clearly demonstrated that the risks to the data subject were new risks caused by the new technology that forms part of the new system. ES feared that any computer action risked to be covered by this provision. FI considered the paragraph too vague and suggested to clarify it in a recital. CY wanted to know what the specific risks were and thought that is should be specified. FR asked that it be made clearer (what risks are associated with new technologies?), and deleted if necessary.

363 HU suggested supplementing Article 26 with a new paragraph (1a) with the following wording: "(1a) In the case of processing referred to in Article 7 (1) a) Member States shall ensure that the legislator consults the supervisory authority prior to the adoption of a law concerning the processing of personal data referred to in paragraph (1)."

1a. In the case of a processing referred to in Article 7(1)(a) Member States shall ensure that the supervisory authority is consulted during the preparation of proposals for legislative or regulatory measures[364] which provide for the processing of personal data referred to in paragraph (1).[365]

2. Member States may provide that the supervisory authority establishes a list[366] of the processing operations which are subject to prior consultation pursuant to paragraph 1. [367]

3. Member States shall[368] provide that where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 does not comply with the provisions adopted pursuant to this Directive, in particular where risks are insufficiently identified or mitigated, the supervisory authority [369] shall within a maximum period of 6 weeks[370] following the request for consultation give advice to the data controller. This period may be extended for a further month, taking into account the complexity of the intended processing. [371]

---

364 FR wanted to remove *regulatory measures* because it was against the procedural autonomy of the MS. DE asked what a *regulatory measure* was. DE meant that the paragraph represented added value if a measure implied a special risk and that the measure must be proportional.

365 CZ and UK scrutiny reservation. SE found that the SA should not be consulted when new legislative proposals were prepared because such proposals were national legislation so in line with the subsidiarity principle this was up to the MS to legislate but if the Directive would be covering domestic processing it would be acceptable. SI on the other hand welcomed the obligation to consult. DE meant that it was necessary to frame the paragraph.

366 CY, EE, FR were of the opinion that it was for the MS to establish such a list. IT thought that it was a good idea to set out riskiness.

367 EE required more flexibility in paragraph 2. CZ was not yet sure whether it considered that paragraph 2 should remain in the text or not. ES did not see any added value of the paragraph and thought it more appropriate to have a prior consultation before legislative activities. UK thought that paragraph 2 made it burdensome for the controller to decide when it was needed to consult the supervisory authority. FR asked for more precision. FR meant that it should also be allowed for Member State legislators to adopt such lists. DE meant that since paragraph 2 was purely declaratory it could be removed.

368 NL wanted to replace *shall* with *may.* Cion said that the text in GDPR used *shall* and wanted to keep it here too.

369 Following IE suggestion.

370 CZ considered that this time limit was too long and meant that 3 weeks would be enough. SE and PT scrutiny reservation on the time limit.

371 FR voiced concerns about the new paragraph 3, because its usefulness and implementation remained unclear. FR considered that the time limit should be extended to two months. UK felt that there were many situation involving law enforcement and intelligence where it would not be appropriate for the SA to comment. SI meant that this paragraph was too prescriptive and wanted its removal. ES found the paragraph not conclusive enough: the deadline could be excessive; what was the effect of the consultation since the consultation was not compulsory (as in the GDPR). NL considered that it was not for the SA; it would be an violation of their independence.

372

SECTION 2

DATA SECURITY

Article 27

Security of processing[373]

1. Having regard to available technology and the costs of implementation and taking into account the nature, context, scope and purposes of the processing **374**and the risks**375** for the rights and freedoms of data subjects**376**, Member States shall provide**377** that the controller and the processor implement appropriate technical and organisational measures to ensure a level of security appropriate to these risks (…).**378**

2. In respect of automated data processing, each Member State shall provide that the controller or processor, following an evaluation of the risks**379**, implements measures designed to**380**:

---

372 DE suggested adding a paragraph for urgent cases as follows: "4. Member States may provide that the controller or processor may consult the supervisory authority without undue delay after the processing referred to in paragraph 1, if otherwise serious disadvantages for the purposes mentioned in Article 1 (1) are expected "

373 DE and FI scrutiny reservation. NL suggested to add Article 30 of the Regulation here. Cion stated that the text was already in the DPFD and that in §2 the Cion had wanted to add extra flexibility. CY found it necessary to clarify the relationship between the controller and the processor, aligning it to the GDPR.

374 PT wanted to delete text from "and" to "data subjects", to address the risks represented by the processing and the nature of the data to be protected and replace it with "the risks represented by the processing and the nature of the data to be protected".

375 FR considered it necessary to better define risk and look at the recitals in GDPR for inspiration.

376 PL pointed to Article 22 in DPFD, whose scope and implementation had not caused any problems. CZ wanted to move the new parts to the end of the paragraph.

377 FR suggested to replace *provide* with *ensure* since this article establishes an obligation to achieve a result, which is, moreover, incompatible a priori with the limits imposed later in the text in relation to technical developments and the cost of their implementation. Support from AT referring to Article 22 in DPFD. Cion could agree to use *ensure* rather than *provide.*

378 ES suggested not to include the principles in paragraph 1 and include the ideas in paragraph 2.

379 FR expressed concerns about the concept of the *evaluation of the risk* and believed that this evaluation should be obligatory only for the processing of the most sensitive types of data, as is the case in the GDPR. DE meant that the criteria and conditions for the risk evaluation were still unclear and stressed that no unnecessary burden should be created.

380 FR stated that a better alignment between paragraph 2 and Article 3(9) defining *personal data breach*, where the concepts of *accidental or unlawful destruction, loss* were worded differently. FR also pointed out that the list of security measures did not seem appropriate for all types of

(b) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);

(c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

(d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

(e) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);

(f) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);

(g) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);

processing, nor all architectures, and that it did not guarantee the technological neutrality of the Directive. FR believed that the specification of the scope of this provision should be kept to a minimum and that the list should be indicative. FR suggested that the list currently given in Article 27(2) should instead be set out in a recital, for instance at the end of the new recital 37b, to provide examples of such measures.

(h) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input (input control);[381]

(i) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);

(j) ensure that installed systems may, in case of interruption, be restored (recovery);

(k) ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored personal data cannot be corrupted by means of a malfunctioning of the system (integrity).

3. (…)[382]

[381] FR pointed out that the reference should be made to Article 24(1) in order to harmonise traceability obligations, rather than create a new obligation here.

[382] Cion reservation on deletion of paragraph 3.

Article 28

Notification of a personal data breach to the supervisory authority[383]

1. Member States shall provide that in the case of a personal data breach <u>which is likely**[384]** to severely affect**[385]** the rights and freedoms of data subjects</u>, the controller notifies**[386]**, without undue delay (…)**[387]** the personal data breach to the supervisory authority (…).

---

383 DE, NO, BG, FI and SI entered scrutiny reservations. Referring to paragraphs 1a and 4, SE said that the notification requirement seemed to be maintained. DK thought that it was not meaningful to report every data breach; it would entail a heavy administrative burden. Support from CY, SE. PL asked if it could be possible that breaches without impact on the data subject could be notified according to a list.UK suggested that only significant breaches(*e.g.* depending on the nature of the data, if mitigation measures have been used) needed to be notified to the supervisory authority. SE also pointed at the far-reaching obligation in Article 28. UK raised concerns about Article 28 because self-incrimination was not protected. EE suggested that Articles 28 and 29 be in line with the relevant Articles in the Regulation. EE also suggested that Article 28 should contain derogations and a risk-based criterion. DE considered that Article 28 went too far. DE meant that it would not be possible to fulfil the requirements in letters (c), (d) and (e) in paragraph 3 within the time frame set out. DE thought that the scope of Article 28 was unclear. DE found it necessary to ensure that the notifications and their handling by the supervisory authorities endanger neither the legitimate interests of third parties nor police and judicial interests. Cion reservation: consistency with the e-Privacy Directive should be kept. UK was concerned that that there may be cases where it could prejudice on-going, sensitive investigations if a law enforcement agency is required to communicate the breach to the DPA. IT suggested a text according to which the controller had to inform the authorities of a violation and check if there is any need to inform the data subject. IT wanted to review the text, especially paragraph 1a, and align it to the text of the GDPR.

384 ES found that *likely* and *severely* created problems for legal certainty and wanted objective criteria.

385 NL and LV asked what a serious breach was: NL and LV suggested to clarify it in a recital and RO to establish criteria for . The Chair pointed to recital 42 that addressed this issue.

386 FR wanted to frame the notification obligation more, *e.g.* referring to potential harm. DE suggested to focus on the risk occurred due to the breach. LV thought that the notification should not be carried out if it risked to interfere with an investigation .

387 CZ suggested to revert to a fixed deadline and like in Article 31.1 extending it to 72h. FR suggested to provide for a two-stage notification process, which would allow more specific *information to be provided at the second stage.*

1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 29(3)(a) and (b). [388]

2. The processor shall alert and inform the controller without undue delay[389] after having become aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least describe the nature of the personal data breach, the likely consequences of the personal data breach identified by the controller, and the measures taken or [390]proposed to be taken by the controller to address the personal data breach.
(…)

4. Member States shall provide that the controller documents any personal data breaches referred to in paragraph 1, comprising the facts surrounding the breach, its effects[391] and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose. [392]

---

[388] NL scrutiny reservation. DE found the legislative technique referring backwards in the text strange and therefore suggested adding the text of Article 29(3) (a) and (b) to this Article. CZ and LV meant that the reference should be made to paragraph 3(c) as well. NL wanted to delete paragraph 1a since it could undermine paragraph 1. SI wanted to delete the paragraph. AT reservation. Cion meant that the paragraph could dilute the obligation to notify and therefore suggested to further develop recital 42 to take account of this.

[389] SI asked whether the timeframe should not be *immediately.* UK preferred the current text.Cion meant that the current text gave enough flexibility.

[390] FR believed that the obligation to propose measures to address any negative consequences of the breach should be mitigated by the insertion of *where appropriate* after *taken.*

[391] FR wanted that the obligation to describe the nature of the data breach be formulated in a more realistic manner and therefore asked for the phrase *identified by the controller* to be added after *its effects*.

[392] NL suggested to delete paragraph 4 due to duplication. DE said that the review must focus on whether the provision risks to create bureaucratic requirements.

393

5. (…)

6. (…)

394

393 HR wanted to insert a new paragraph 4a with the following wording: "(4a) Competent authority monitors the protection of personal data at the request of the respondents, on a proposal from a third party or ex officio." DE suggested to insert the following new paragraph because the obligation to incriminate oneself could be problematic in terms of fundamental rights "4a. In the event that proceedings must be brought against a controller or processor on account of a violation of duty which necessitates the measures under Articles 28 or 29, Member States may provide that the measures taken by the controller and processor under Article 28 and 29 may not be used in these proceedings."

394 BE suggested inserting an Article 28a with the following heading " Communication of the data breach to the concerned Member States' controllers" and the following text: "1. Member States shall provide that in the case of a personal data breach which is likely to severely affect the rights and freedoms of data subjects, the controller from a MS where the breach happened notifies, without undue delay (...) the personal data breach to the controller of the MS from which the data are originated or have been transferred to (...).

2. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 29(3)(a) and (b).
3. The notification referred to in paragraph 1 shall at least describe the nature of the personal data breach, the likely consequences of the personal data breach identified by the controller, and the measures taken or proposed to be taken by the controller to address the personal data breach. (...)
4. Member States shall provide that the controller from the MS where the breach happened documents any personal data breaches referred to in paragraph 1, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the controller of the MS from which the data are originated to take the first measure in order to limit the breach. The documentation shall only include the information necessary for that purpose".

Article 29

Communication of a personal data breach to the data subject[395] *396*

[395] BE, CZ, DE, EE, FI, NO, SI scrutiny reservations. ES and PTsuggested to delete Article 29, ES because it represented a risk for the security and PT because the communication should be indirect in criminal proceedings. SI objected to the deletion and stated that it could be necessary for the right of defence (judicial right). NL also saw a problem informing the data subject of a breach and was generally hesitant to the need to notify the data subject. FR was sceptical to the new changes compared to the text in DPFD, *e.g.* paragraph 1 was redundant. FR wondered if it was necessary to notify only the supervisory authority. Support from ES, NL. EE wanted to know how the Article 29 could work in the context of a Directive. DE asked whether such an obligation could work in the public sector and expressed a certain scepticism. DE also cautioned against bureaucracy. Cion reservation: consistency with the e-Privacy Directive should be kept. UK urged strongly for an exemption to this in situations where communicating the breach to the data subject might prejudice an investigation. CY also raised concerns about the interference with ongoing investigations. AT asked how to strike the right balance between supervision/communication to the data subject and the protection of fundamental rights. FR, supported by CH, asked that the communication provided for in this article be limited to data subjects who have the right of information over their personal data. FR also believed that this article, like those relating to data subjects' rights in Chapter III, should establish the principle of the absence of notification, except:
where the personal data affected by the security breach relate to a data subject with the right of information, in cases which do not fall within the restrictions of data subjects' rights allowed by our proposal for Article 10; and where the security breach is particularly harmful to the data subject's rights and freedoms. FR therefore suggested the following drafting for Article 29:
"Article 29
Communication of a personal data breach to the data subject

1. The communication of a personal data breach to the data subject may be delayed, restricted or omitted on the grounds referred to in Article 10.
2. When the communication of a personal data breach is not restricted or omitted according to paragraph 1 and subject to paragraphs 3 and 4 of this Article, Member States shall provide that when the personal data breach is likely to severely affect the rights and freedoms (…) of the data subject, the supervisory shall, after the notification referred to in Article 28, communicate the personal data breach to the data subject without undue delay.
3. The communication to the data subject referred to in paragraph 2 shall describe the nature of the personal data breach (…).
4. The communication (…) to the data subject referred to in paragraph 2 shall not be required if:

(a) the controller (…) has implemented appropriate technological protection measures, and those measures were applied to the personal data affected by the personal data breach in particular those that render the data unintelligible to any person who is not authorised to access it; or
(b) the controller has taken subsequent measures which ensure that the data subjects' rights and freedoms are no longer likely to be severely affected; or
(c) it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner."

[396] DE thought that it was necessary to examine for example if the requirements set out in Article 29 could be applied to the public sector (police and judicial authorities), whether "negative publicity" can have impacts on security authorities similar to those in the public sector and to determine the

1. Subject to paragraphs 3 and 4 of this Article, Member States shall provide that when the personal data breach is likely to severely affect the rights and freedoms (…) of the data subject, the controller shall, after the notification referred to in Article 28, communicate the personal data breach to the data subject without undue delay. [397]

2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach (…).

3. The communication (…)[398] to the data subject[399] referred to in paragraph 1 shall not be required if:

(a) the controller (…) has implemented appropriate technological protection measures, and those measures were applied to the personal data affected by the personal data breach in particular those that render the data unintelligible to any person who is not authorised to access it; or

(b) the controller has taken subsequent measures which ensure that the data subjects' rights and freedoms are no longer likely to be severely affected[400]; or

---

extent to which notifying data subjects would interfere with the work of the police and judicial authorities.

397 BE, BG required more specific criteria in paragraph 1. NL reservation. NL and SK meant that is should not be mandatory to notify the data subject. NL further thought that if a data breach had occurred in many MS measures within The SIS system would need to be taken.

398 DE suggested to insert the content of Article 29.3(a) and (b) into Article28.1a, if this will be the case then a reference to Article 28.1a would be necessary.

399 FR wanted a clarification of what *communication to the data subject* meant, and of the differences between this and *the information to the data subject*. If these two expressions meant the same thing, the same terms should be used.

400 NL did not see the difference between paragraphs (a) and (b) and suggested to merge the texts.

[(c) it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.][401]

4. The communication to the data subject referred to in paragraph 1 may be delayed, restricted or omitted [402] on the grounds referred to in Article 11b[403].

[404]

[405]

[401] DE, LV, CH, ES, CZ, IT and SI wanted to maintain the text in brackets in the text. SE asked if it was acceptable to require communication to the data subject when there was no obligation to notify him or her (29.3(c)). In the same vein FR and BE that meant that it was enough to inform only the data subject that had the right to be informed and not all data subjects. BE added that with the indirect access the data subject never knows.

[402] IE suggested to replace *omitted* with *excluded* or *dispensed with.*

[403] ES suggested to add references to paragraphs (c) and (d) as well so that other potential grounds for exceptions be included.

[404] BE and NL suggested inserting a new paragraph 5 with the following wording: "Member States may determine by law categories of data processing which may wholly or partly fall under the grounds referred to in paragraph 4." FR positive scrutiny reservation.

[405] BE and NL suggested inserting a new paragraph with the following wording: " Member States shall provide that where the data breach involves personal data that have been transmitted by another Member State, the information, meant in Article 28(3), will be communicated to this Member State without undue delay".

SECTION 3

DATA PROTECTION OFFICER [406]

Article 30

Designation of the data protection officer[407]

1. Union law[408] or Member State law may[409] provide that the controller or the processor designates a data protection officer.

2. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 32. [410]

---

406 PT wanted to delete the whole section 3 because a DPO would not be bound by the professional secrecy and should not have access to all information. Introducing a DPA in PT law would entail constitutional problems. For PL it was important that the DPO acted independently in order to carry out the tasks properly.

407 DE, EE, FI, NO and SI scrutiny reservations. SI considered that only criteria could be set out. DK asked whether "shall provide ..." could refer to collective agreements as well Referring in particular to paragraphs 2 and 3, PL preferred not having so many details on the designation of a DPO. BE wanted to add an Article setting out that rules on professional secrecy should be applicable to the DPO. Cion declared itself willing to look into this but it saw two problems linked to it: Article 32(h) on the DPO acting as a contact point should not be limited; if no reference was made to the DPO it could be an external person. DE thought that it would be useful to examine whether additional instruments to protect government data protection officers should be adopted or whether rules for data protection officers in Article 35.7-10 in GDPR should be included in the Directive.

408 For the NL it was problematic to refer to EU law and SI asked why there was such a reference. Cion informed that this referred to Article 28 in the Europol Decision and Article 17 of the Eurojust Decision. DE wanted to delete the reference to *Union law*.

409 Cion reservation on replacing the mandatory DPO by an optional DPO. DE and NL supported that the designation of a DPO should be mandatory since it was important to have harmonised rules on this. Cion stated that if the designation of a DPO was voluntary it would be necessary to harmonise the tasks. ES informed that in the context of the examination of the Regulation it had defended a voluntary DPO and did so for the Directive as well.

410 FR raised doubts about Article 31 and also concerning the independence. Cion replied that the three Articles were inserted to ensure consistency with the Regulation. Independence in the police sector should not be a problem, one could look at the situation in DE, Europol and Eurojust. Cion said that a DPO could be shared, it could also be a part time job and could be based on a contract. CH and PL wanted to delete paragraph 2.

3. A single data protection officer may be designated for several competent public[411] authorities, taking account of their organisational structure (…) and size. [412]

4. *Member States shall[413] provide that the controller or the processor ensures that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.*

[411] BE suggested to delete *public* because some competent authorities are not public in BE. NL preferred the initial text.

[412] PL wanted to delete paragraph 3 because it considered that the Directive only should contain overarching rules and it should be left the MS to set out the details.

[413] CH suggested to replace "shall" by "may".

5. *The controller or processor shall ensure that the data protection officer is provided with the means to perform (…) the tasks referred to under Article 32 effectively and can act in an independent manner with respect to the performance of his or her tasks (…).* [414]

[415]

Article 31

Position of the data protection officer

(…) [416]

Article 32

Tasks of the data protection officer[417]

Member States shall[418] provide that the controller or the processor entrusts the data protection officer (…) with the following tasks:

(a) to inform and advise the controller or the processor of their obligations in accordance with the provisions adopted pursuant to this Directive (…); [419]

[414] CH wanted to remove paragraph 5. SE while supporting the deletion of Article 31 noted that part of its content had been moved to Article 30.5 which it could support.

[415] BE suggested the inserting of a paragraph 6 as follows: "The data protection officer shall, both during and after his/her term of office, be subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties".

[416] DE suggested adding the following text: " The data protection officer shall suffer no disadvantage through the performance of his duties."

[417] DE, EE, FI, FR, NO, SI scrutiny reservations. NO, SE and EE considered the Article too detailed.

[418] CH wanted to replace "shall" by "may" because it was contradictory to have a mandatory provision here when the designation of a DPO in Article 30 was voluntary.

[419] NL found that the text was not so well drafted.

(b) to monitor compliance with provisions adopted pursuant to this Directive and with (…) the policies[420] in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations and the related audits; [421]

(c) (…)

(d) (…)

(e) (…)

(f) (…)

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, to co-operate with the supervisory authority at the latter's request or on his or her own initiative;

(h) to act as the contact point for the supervisory authority on issues related to the processing of personal data and consult[422], (…) as appropriate, on any other matter (…).

[423]

[420] RO wanted to add "of the controller or processor" between *policies* and *in relation to.*

[421] SE asked how this paragraph was related to external audits. CH suggested removing paragraphs (b) - (g).

[422] DE wanted it to be clarified whether the consultation referred to was the prior consultation in Article 26 or if it referred to a general option of proactively consulting the SA.

[423] FR asked for the insertion of an additional point to be added to the list of tasks in paragraph 1, to provide that the data protection officer should produce an annual report to submit to the controller.

CHAPTER V

TRANSFER[424] OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS [425]

Article 33

General principles for transfers of personal data [426]

---

424 FR found it necessary to define *transfer.*

425 AT, BE, CH, CZ, CY, DE, DK, EE, FI, FR, IT, NL, NO, PL, PT, RO, SI, UK scrutiny reservation on Chapter V. ES reservation on Chapter V.DE questioned whether the core concept in Chapter V was appropriate and adequacy danger. SE stressed that administrative rules must not make transfer to third countries and international organisations more difficult. FI wanted that the content of Article 14 (transmission to private parties in MS) should be covered in the future as well. FR and BE meant that it was necessary to link Chapter V and Article 60. BE said that its scrutiny reservation was linked to the uncertainty of the role and statute of international organisations in general and Interpol in particular. It was important for BE that the MS could continue to cooperate as they do now. For CZ swift and efficient international information exchange was an important precondition for the protection of fundamental rights by preventing and combating crime. ES raised concernes about the competences assumed by the Commssion in this chapter, which may directly or indirectly affect to security issues that belong to Member States, ES thererfore considered that the potential political impact of Article 34.5 should be carefully assessed. FR was in favour of maintaining the adequacy procedure but meant that is was necessary to preserve the procedures in Articles 35 and 36 since they would be most used by the MS allowing them to continue to exchange data with third countries, due to the low number of adequacy decisions taken on basis of Directive 95/46 and the absence of such a procedure in the DPFD. FR meant that Article 35 should be viewed as enabling MS to maintain exchange with third countries channels with third countries in the absence of adequacy decisions. FR said that it could be necessary to exchange data with third countries not offering an adequate level of protection and that the operational needs required to allow such exchanges must be continued to be carried out. AT wanted that the sequancing of the transfer in Chapter V should be made clear, *i.d.*positive adequacy decision, if no adequacy decision the need for the MS to assess the safeguards offered and in the third place a transfer in the individual case in exceptional circumstances. AT also wanted it to be clarified which possible appropriate safeguards within the meaning of Article 35 could result in a transfer despite a negative adequacy decision. SE wanted that Chapter V be simplified and that it must be clear how the different Articles were related to each other, *e.g.* must the conditions in Article 33 be complied with for transfers based on Articles 34 and 35 and when Article 36 was applied. SE asked whether the possibilities to transfer data were not too limited in the draft text, *e.g.* transfer of data for judicial administratice proceedings with a direct link to combating crime, not even after consent from the initial MS.

426 PT wanted to see more safeguards in Article 34. The Chair indicated that the equivalent Article had been deleted in the GDPR. AT, FI and PT were against a deletion of Article 33 because the content of Article 13 in DPFD would not be covered. SI was sceptical about the deletion. In contrast BE, CZ, ~~EE~~, SE supported the deletion. CH, FR entered scrutiny reservations on the possible deletion of Article 33. DE said that the Article did not set out criteria for striking the right balance between data protection and investigation and prosecution of crime. DE criticized that the

Member States shall provide that any transfer of personal data by competent public authorities (…) to a third country, or to an international organisation[427], including further onward transfer to another third country or international organisation, may take place only if [428]: [429]

(a) the transfer is necessary for the prevention, investigation, detection or prosecution of [430] criminal offences or the execution of [431] criminal penalties; [432] and[433]

Directive was drafted in a way that it was not possible to know what was the main rule and which were the exceptions. EE, PL, SE, SI and UK welcomed DE comments about the right balance between data protection and combating crime. DE scrutiny reservation because the scope remained controversial. SE asked how the different Articles in Chapter V were linked and AT how Chapter V fitted into the overall scheme. CZ noted that the corresponding Article had been removed from the GDPR and asked for its deletion here as well. CZ considered the Article too vague and confusing, and the following problems would arise: Data transfers to victims (or supportive organizations) were probably prohibited, which would be contradictory to the Victims Directive 2012/29/EU; Data transfers to Interpol and international tribunals were put in doubt (the wording "international organizations" was stricter than that of Article 13 DPFD, which spoke about *bodies);* Purposes (a) were excessively limited (appropriate reference to "maintenance of public order" must be included and further purposes must be examined); The relation to Article 36 and 36a was not clear (a reference to Article 36 should be added in point(e) or (e) could be rephrased, in addition a reference to Article 36a should be added in point (d), a possibility to impose a deadline for the Member State from which personal data originated to give its prior authorization should be considered); CZ could also consider copying Article 13 in DPFD. ES meant that the approach of this article was misleading because it looked like international transfers were only possible on the basis of an adequacy decision or appropriate safeguards. ES said that this approach was clearly compromised by Article 36 and ES preferred a more realistic approach. AT wanted that it be ensured that the third State used the data only for the isolated case for which the data were transferred, and that subsequent transfer and/or use for other purposes required the consent of the transferring State and - if the data originally came from another Member State - of the "State of origin" of the data.

427 FR asked for clarifications as to which organisations were intended. BE meant that the role and status of international organisations should be clarified. Cion accepted to clarify the meaning of *international organisation.* FR asked about the relationship between this Directive and those organisations' specific rules on data protection.

428 DE suggested to add the following text after "only if" "in addition to the conditions under Article 7" for the sake of legal clarity, including the paragraph 1a (consent by the data subject) suggested by DE

429 ES considered that the text "may take place only if" needed to be redrafted.

430 AT suggested to add "a specific" before criminal offence in order to clarify that transfer may only take place in a specific case and not as a routine transfer.

431 AT suggested to add "a specific" before criminal penalty in order to clarify that transfer may only take place in a specific case and not as a routine transfer.

432 DE asked whether paragraph (a) could be used outside the purpose of police work, for example in the context of asylum or immigration law. CZ supported that the asylum and immigration law be covered by the Directive. The purpose must be set out in the Directive according to DE. CZ wished to insert a reference to Article 1(1) in paragraph (a) as had been done in paragraph (c).

433 BE suggested to replace *and* with *or* and add the following paragraph "(b) the transfer is necessary for the prevention of criminal offences and in maintaining public order and security for

(b) (…)

(c) the controller in the third country or international organisation[434] is an authority[435] competent for the purposes referred to in Article 1(1); and

(d) in case personal data are transmitted or made available from another Member State,[436] that Member State has given its prior authorisation[437] to the transfer [438] in compliance with its national law[439]; [440] and

major events, in particular for sporting events or European Council meetings; and" The suggestion comes from Article 14 of the Council Decision 2008/615/JHA Prüm Decision. DE suggested to remove paragraph 1(a) to avoid that the relationship with Article 7 was unclear.

[434] NL asked how paragraph (c) tied in with international organisations in criminal prosecution.. Cion accepted to clarify the meaning of *international organisation.* FI thought that paragraphs (c) and (e) needed to be fine tuned and that Interpol should be covered. FI suggested to use *intergovernmental organisation* in accordance with the Vienna Convention on the Law of Treaties. FI thought that the organisations should be set out here, *i.d.* Interpol or that it be made clear in the recitals that Interpol was covered.

[435] DE suggested to delete paragraph (c) and revise recital 45 so as not to rule out the possibility for judicial authorities and the police to share information with private parties, this is in particular important for cybercrime.

[436] EE said that it sometimes was difficult to know that data had arrived from a third country.

[437] DE understood "prior authorisation" to cover authorisations given for transfers within the EU or generally and meant that this should be set out in recital 49a, as was the case in recital 24 in FDDP.

[438] AT wanted to add "including further onward transfer," after *transfer* to make clear that the consent in also necessary for subsequent transfer.

[439] EE thought that paragraph (d) should be linked to Article 36a.

[440] AT suggested to insert another principle after point (d) that transfers may take place only if and insofar as provided for in national law.

(e) the Commission has decided pursuant to Article 34[441] that the third country or international organisation[442] in question ensures an adequate level of protection or where appropriate safeguards are adduced or exist in accordance with Article 35.[443]

[444]

[441] AT meant that it was necessary to make a reference to all types of transfer provided for in Chapter V, including Article 36 in order to make it clear that the general basic principles set out in Article 33 (particularly points (c) and (d)) are also fully applicable to transfers referred to in Article 36. Support from FR to mention Article 36.

[442] FR asked for clarifications as to which organisations were intended. BE meant that the role and status of international organisations should be clarified. Cion accepted to clarify the meaning of *international organisation.* FI thought that paragraphs (c) and (e) needed to be fine tuned and that Interpol should be covered. FI suggested to use *intergovernmental organisation* in accordance with the Vienna Convention on the Law of Treaties. FI thought that the organisations should be set out here, *i.d.* Interpol or that it be made clear in the recitals that Interpol was covered.

[443] ES queried whether paragraph (e) did not contradict Article 36 whereas CH, FR, UK suggested to insert a reference to Article 36. NL asked about cooperation agreements with third countries for *i.d.* investigation but that the data could be used in the third country for other purposes than those sat out in paragraph (e). NL suggested to insert *consent* to be able to use the data for all purposes. FI meant that, in line with Article 34, a territory or specified sector within a specific third country should be mentioned in paragraph (e). DE wanted to add "or where the personal data are transferred in accordance with Article 36" in the end of paragraph (e) to clarify that Article 36, as well as Articles 34 and 35 can serve as grounds for data transfer.

[444] DE suggested to insert a paragraph 2 with the following wording: "(2) Member States shall provide that the recipient shall be informed of any processing restrictions and be notified that the personal data may be used only for the purposes for which they are transferred. The use for other purposes shall be allowed only with the prior authorisation of the transmitting member state and, in case personal data had been transmitted or made available from another member state to the transmitting member state, the prior authorisation of the other member state too, or in cases where the requirements of Article 36a are fulfilled". DE had taken this text from removed Article 37 because it found it important as it is a general principle for transfer to third countries, however the part on *reasonable steps* had been deleted. DE found it also important that use for other purposes could only be carried out with the consent of the transferring MS, maybe also the MS from where the data originated (like in Article 33.1 (d).

Article 34

Transfers with an adequacy decision [445]

1. Member States shall provide that a transfer[446] of personal data to a **(...)** third country or an international organisation may take place where the Commission has decided in accordance with Article 41 of Regulation (EU) …./2012 or in accordance with paragraph 3 of this Article that the third country or a territory or a **specified** sector[447] within that third country, or the international organisation[448] in question ensures an adequate level of protection[449]. Such transfer shall not require any specific authorisation. [450]

---

445 DE scrutiny reservation. CH said that in case the GDPR should not constitute an integral part of the Schengen acquis, CH would not be bound by its provisions. However, in order to avoid restrictions in data exchange, CH should continue to be considered a Schengen country regarding the exchange of data between EU MS and CH in the entire area of Schengen and Dublin cooperation. This includes data exchange under the Schengen and Dublin cooperation to which the Data Protection Directive does not apply. DE had doubts if Article 34 corresponded with reality. DE further did not support the Cion's role regarding adequacy decisions. UK supported DE that it was better that the adequacy decision were taken by the MS rather than Cion. DE said that Article 60 and Article 34 were contradictory. ES considered that consistency between the text of GDPR and Article 34 must be ensured so that the adequacy functioned in an equivalent manner. FR wanted a clarification concerning the procedure for adopting an adequacy decision, will it be the same as the current system, *i.e* Article 31 of Directive 1995, and who can refer a matter to the Cion.

446 BE and FR suggested to talk about "any transfer or set of transfer" .BE and FR suggestion.

447 The term processing sector was changed to specified sector in Chapter V of GDPR, as agreed at the Council in June 2014. FR asked for example if a State could not be subject of an adequacy decision whereas one of its entities might be, or that an international organisation might ensure an adequate level in one sector but not in another.

448 FR thought that the *international organisations* could be deleted in this paragraph.

449 For SE it was important that the procedure to adopt a Decision on an adequate level of protection was not made too complicated. (FI wanted that adequacy decisions must be made swifter than currently.) FR asked about the meaning of the last sentence of paragraph 1. NL pointed to the low number of countries being considered as having an adequate level of protection by the Cion and meant that a heavy procedure was being created. NL wanted Cion to explain how this procedure would be used for the police and judiciary sectors.

450 BE asked whether the individual MS could have additional requirements. PL meant that since law enforcement authorities would need to react quickly to protect *e.g.* fundamental rights, if there was a general decision by the Cion that would not be possible. DE meant that since *authorisation* could lead to misunderstandings it should be deleted and the following wording be added: " additional assessment in respect of the level of data protection. Decisions taken by the Commission under sentence 1 shall not result in an obligation of Member States to transfer data". With this wording DE also wanted to make clear that there is no obligation to transfer data.

2. Where no decision adopted in accordance with Article 41 of Regulation (EU) …./2012 exists, the Commission [451] shall[452] assess the adequacy of the level of protection, giving consideration to the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, data protection rules (…)[453] including concerning public security, defence, national security and[454] criminal law as well as the security measures, including rules for onward transfer of personal data to another third country or international organisation,[455] which are complied with in that country or by that international organisation; as well as the existence of effective and enforceable data subject rights and (…) effective administrative and judicial redress for data subjects (…) whose personal data are being transferred; [456]

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility (…) for ensuring compliance with the data protection rules, for assisting and advising (…) data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States[457]; and

---

451 RO meant that it was necessary to involve the EDPB at this stage.

452 DE suggested to replace *may* with *shall* because it seemed excessive and undesirable that the Cion had to assess the level of protection of all countries in the world and if the Cion found that a country did not have an adequate level of protection it would entail political tensions, DE therefore found it better to leave it to the Cion to decide whether or not to assess the level of protection.

453 DE preferred the Cion text, deleting "data protection rules" and adding "in force, both general and sectoral" after *relevant legislation.*

454 DE wanted to delete *and.*

455 DE preferred the text in the Cion proposal, that is deleting the underlined text from *including* to *organisation.*

456 Cion meant that the equivalent text to Article 34.1(a) was clearer in the GDPR (Article 41.2(a).

457 Cion scrutiny reservation.

(c) the international commitments the third country or international organisation concerned has entered into, **or other obligations arising from its participation in multilateral or regional systems, in particular** [458] in relation to the protection of personal data. [459]

[460]

2a. The European Data Protection Board shall give the Commission an opinion for the assessment of the adequacy of the level of protection in a third country or international organization, including for the assessment whether a third country or the territory or the international organization or the specified sector no longer ensures an adequate level of protection.

3. The Commission after assessing the adequacy of the level of protection, may decide, within the scope of this Directive, that a third country or a territory or a **specified** sector within that third country or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 57(2). [461]

4. (…)

4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3.

---

[458] DE also here wanted a broader assessment, like in paragraph (a) and therefore suggested adding *especially* before *in relation.* FR asked whether it might not be worth including the agreements and international conventions to which the Union is party, because they must as least be presumed having an adequate level of protection, *e.g.* CoE Convention 108.

[459] DE asked what protection level must be kept. Cion reservation.

[460] DE wanted to add the following text: " The Commission shall, as early as possible, give the Member States the opportunity to comment on each adequacy assessment." because it wanted the MS to be able to comment early in the process.

[461] NL wanted to know how this paragraph would be applied. CZ meant that paragraph 3 should include a duty for the Commission to seek opinion of the EDPB and thought that the role of the EDPB should be the same as in the GDPR. CZ wanted that Paragraph 3 should include possibility of Member States to adopt adequacy decision as well (Article 13 in DPFD.

5. The Commission may decide within the scope of this Directive that a third country or a territory or a **specified** sector within that third country or an international organisation [462] no longer ensures an adequate level of protection within the meaning of paragraph 2, and may, where necessary, repeal, amend or suspend such decision without retro-active effect.[463] The (…) implementing acts shall be adopted in accordance with the examination procedure referred to in Article 57(2), or, in cases of extreme urgency, in accordance with the procedure referred to in Article 57(3)[464]. *At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision* (…).[465]

5a. The Commission shall enter int consultations with the third counrty or international organisation with a view to remedying the situation giving rise to the Decision made pursuant to paragraph 5.

[462] AT suggest to add the following text to allow the Cion to issue a negative adequacy decision "or an international organisation *does not ensure* an adequate level of protection within the meaning of paragraph 2, and may, where necessary, repeal, amend or suspend such *prior* decision without retro-active effect."

[463] FR thought that it could be made clearer that the repeal of adequacy decisions were based on monitoring by the Cion, as is provided in paragraph 4a and that it is only if the third country changes its legislation or its practice.

[464] DE saw no need for an immediately applicable implementing acts and therefore suggested to delete the text after *57(2)*until *57(3).*

[465] BE, CH, CZ, DE, FR, NL, SE welcomed the Chair's suggestion to remove paragraphs 5 and 6 on the blacklist. HU preferred the text of the GDPR and the obligation for the Cion to request the opinion of the EDPB and take its opinion into account. CZ meant that paragraph 3 should include a duty of the Commission to seek opinion of the EDPB. CZ wanted that Paragraph 5 included possibility of Member States to adopt adequacy decision as well. ES found it advisable to better assess what impact this may have on the basis of arts. 35 and 36. ES asked if a decision based on this paragraph would prevent, in general terms, a transfer based on Articles 35 and 36. ES would not be in favor of granting the Commission an inderect way to constraint transfers based on Articles 35 and 36.

6. Member States shall ensure that where a decision pursuant to paragraph 5 is taken, such decision (…) shall be without prejudice to transfers of personal data to the third country, or the territory or **specified** sector within that third country, or the international organisation in question pursuant to Articles 35[466] and 36 (…).[467]

7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and **specified** sectors within a third country and international organisations in respect of which decisions have been taken pursuant to paragraphs 3 and 5.[468]

8. (…)

[466] AT said that if a negative adequacy decision had been taken, a transfer under Article 35 could not be envisaged so therefore should the reference to Article 34 be deleted.

[467] PL asked how paragraph 6 was linked to a situation where no adequacy decision existed. PL also asked if the controller could set up additional requirements. NL did not see any added value of this paragraph and suggested to delete it or making a link to the EDPB.

[468] LV thought that such lists could be published on MS websites. Cion could accept this. CZ thought that there should be a provision requiring the Member States to either publish their adequacy decisions or report them to the Commission. RO did not want the list to contain the countries whose level of protection were not considered adequate (black list) but wanted the Cion to look over and update the list periodically.

Article 35

Transfers by way of appropriate safeguards[469]

1. (…) Member States shall provide that a transfer[470] of personal data to a third country or an international organisationmay take place where: [471]

   (a) appropriate safeguards[472] with respect to the protection of personal data[473] have been adduced in a legally binding instrument[474]; or

---

469 EE asked what would happen after the transfer. CZ and FR meant that the MS must be able to conclude bilateral and multilateral agreements. BE queried whether INTERPOL fell within the scope of Article 35 and asked if INTERPOL Rules on Processing of Data ensure an adequate level of protection, BE hoped that a pragmatic approach would be taken on this issue. Cion said that *Interpol* would be falling under both paragraphs 1(a)and (b).
BE meant that in order to preserve the coherence between this proposal and the proposal of Regulation on the establishment of the European Public Prosecutor's Office, BE would like to give the possibilities to MS to exchange the information via INTERPOL on the same conditions than those provided in art 54 of that Regulation ("Personal data shall only be transferred by the European Public Prosecutor's Office to third countries, international organizations, and Interpol if this is necessary for preventing and combating offences that fall under the competence of the European Public Prosecutor's Office and in accordance with this Regulation.")

470 To align with the GDPR. BE asked to replace *transfer* with *any transfer*. FR preferred to use the plural, *transfers* to make it possible to set up channels for regular and routine data exchange. . IE said that Article 35 and 36 should apply to a category of transfers as well as to a single transfer (Article 44 of GDPR).

471 AT wanted to reinsert the Cion initial text for the *chapeau.*

472 HU asked what appropriate safeguards was and meant that it could not be a uniform compliance here.

473 DE meant that it was important that the criteria in Article 34(2) be applied as well and suggested adding the following text after *personal data* "taking account of the criteria set out in Article 34 (2),"

474 LV, RO, SE and SI asked clarifications on "a legally binding instrument". Cion replied that bilateral legally binding agreements were covered. BE asked whether the general regulations of Interpol would be covered here. CZ suggested to add "such as an agreement concluded by Member State" before *or* to recognize the powers of the individual MS to conclude agreements in this area.

(b) the controller (…) has assessed all the circumstances[475] surrounding [476]transfer of personal data [477] and concludes that appropriate safeguards exist with respect to the protection of personal data. [478]

2. (…) Transfers under paragraph 1 (b) must[479] be (…) documented and the documentation[480] must be made available to the supervisory authority on request. [481]

---

[475] FI suggested that the *circumstances* to be taken into account at the assessment be clearly specified in the Article. Another option according to FI would be to stipulate in line with Article 13.3 of DPFD that the safeguards have been deemed adequate by the MS concerned according to its national law.

[476] DE suggested adding "the individual case of" after *surrounding.*

[477] DE meant that it was important that the criteria in Article 34(2) be applied as well and suggested adding the following text after *personal data* "taking account of the criteria set out in Article 34 (2),"

[478] NL had doubts about the need to keep Article 36.1(b). NL, AT, HU and RO scrutiny reservation on Article 35.1(b). UK thought that it was not clear whether every single processing operation needed safeguards or whether it was more general.

[479] BE suggested to replace *must* with *shall, as far as possible, .*

[480] ES asked for clarifications on what was meant with *documentation* and asked if all aspects of paragraph 1(b) were covered. ES worried that the documentation obligation would impact legal proceedings and procedural laws. ES suggested replacing *documented* with "registered" and to replace *documentation* with "records" so as to have a more tech-friendly and future-oriented language.

[481] DE, AT and RO considered the paragraph superfluous since the general documentation requirements in Article 23, for AT Articles 23 in conjunction with Article 18, already applies. HU wanted the text in Article 42.2 in the GDPR and Article 35 in the Directive be consistent and therefore suggested to insert that prior authorisation by the SA would replace the safeguards indicated in the beginning of the paragraph. UK thought that paragraph 2 represented an administrative burden. Cion could accept a broad notion of transfer but the transfer should be documented. DE asked what links existed between Article 35.2 and Article 18.1. FR wanted that a decision on transfer taken by a MS concerning a third country or international organisation should constitute a general transfer towards that state or entity so as to avoid the need to take a new decision for every transfer. SE asked whether this paragraph was still needed after the deletion of parts of Article 35.

Article 36

Derogations for specific situations[482]

(…) Member States shall provide that,[483] in the absence of an adequacy decision pursuant to Article 34 or appropriate safeguards pursuant to Article 35[484], a transfer **or a category of transfers** [485] of personal data to a third country or an international organisation may take place only on condition that [486]:

(a) the transfer is necessary in order to protect the vital interests of the data subject or another person; or

(b) the transfer is necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; or

(c) the transfer of the data is essential[487] for the prevention[488] of an immediate[489] and serious threat to public security of a Member State or a third country; or

---

482 UK and CZ asked why the derogations could not be set out as permissions and be further specified. Likewise, DE welcomed this but considered that they should not be set out as derogations. DE also saw the need for complementing the list. NL saw the need for a better balance. ES and UK did not approve of the title of the Article. BE asked whether each individual transfer would be assessed or if it was for different groups/purposes. IE said that Article 35 and 36 should apply to a category of transfers s well as to a single transfer (se Article 44 of GDPR). NL considered that the EDPB should ensure consistency. CZ thought that it could be good to transfer data to a natural person in a third country and suggested to add text to this effect. ES suggested including the need of keeping records of the transfers under this Article, with a simmilar approach as the one contained in paragraph 2 of Article 35. DE wanted to change the title to "Transfers after weighing of interests" to take account of the interests existing in practice that is data protection interests and *e.g.* the public interest of preventing and solving crimes. AT found tht the wording of Article 36, in particular points (c) to (e) was too broad and preferred to revert to the wording of Article 13(3) of DPFD that takes account of the derogations of Article 2 of the Additional Protocol to CoE Convention 108. AT thought that Article 36 should stipulate clearly that legislation is to provide for such transfers on the basis of *prevailing* public interests.

483 AT noted that in recital 49 it referred to *specific situations* but that those words were missing in the Article and therefore suggested to insert them.

484 AT meant that the introductory phrase should make clear that a transfer under Article 36 can be considered only when a transfer is not already permitted under Article 34 or 35.

485 To align with the GDPR.

486 DE suggested to draft the *chapeau* in the following way, in line with Articles 34 and 35, to indicate that Article 36 was on equal footing with Articles 34 and 35 and should not only set out derogations: "1.(…) Member States shall provide that, a transfer of personal data to a **recipient or recipients in a** third country or an international organisation may take place **"**. DE used *recipient* to indicate that transfers also could go to private bodies.

487 UK preferred to replace essential" with "necessary".

488 CZ said that paragraph (c) should refer to all purposes in Article 1.1, not only prevention.

(d) the transfer is necessary[490] in individual cases for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; or[491]

(e) the transfer is necessary[492] in individual cases[493] for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal penalty. [494]

495

496

---

489 ES suggested to replace "immediate" because this word is often misinterpreted and replace it with "direct".

490 CZ wanted to exchange *necessary* to *essential* as in paragraph (c) or *required* because the meaning of necessary was unclear.

491 CZ asked what documents would be needed for *e.g.* an EAW being transferred to Interpol.

492 CZ wanted to replace *necessary* to *essential* as in paragraph (c) or *required* because the meaning of necessary was unclear.

493 UK feared that *individual cases* could be interpreted narrowly and therefore suggested to delete these words and explain in the recitals.

494 PL suggested that the *chapeau of the Article* and paragraphs (a) to (e) would form Article 36(1) and that a new paragraph 2 would be added with the following wording: "2. Transfers under paragraph 1 must be documented and the documentation must be made available to the supervisory authority on request"

495 DE suggested adding a paragraph (f) with the following wording: "**(**f) the transfer is necessary in individual cases for compliance with a legal obligation or for the lawful exercise of a legal power the controller is subject to." The text from DE was the same as for Article 7(1)(b). CH suggested inserting a paragraph (f) with the following text: "(f) the data subject has given his or her consent to the transfer of his or her personal data for one or more specific purposes." (this could be used when the transfer is in the interest of the victim).

496 DE suggested adding a paragraph (2) with the following wording: "2. Personal data shall not be transferred, if in the individual case the data subject has protectable interests, especially data protection interests, in the exclusion of the transfer, which override the public interest in the transfer set out in paragraph 1."

Article 36a

Transfers without prior authorisation by another Member State[497]

Member States shall provide that transfers without the prior authorisation by another Member State in accordance with point (d) of Article 33 shall be permitted only if the transfer of the personal data is essential[498] for the prevention of an immediate[499] and serious threat to public security of a Member State or a third country or to essential interests[500] of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

Article 37

Specific conditions for the transfer of personal data

(…)

497 Cion reservation on the title. DE meant that for reasons of clarity and systematics it would be preferable to introduce Article 36a into Article 33. AT said that it must be made clear that transfer under this provision without prior consent is ruled out when the Member State in question has previously expressly denied consent.

498 UK preferred "necessary" to "essential".

499 ES suggested to replace "immediate" because this word is often misinterpreted and replace it with "direct".

500 BE asked about the meaning of *essential interest* and whether a common definition existed.

Article 38

International co-operation for the protection of personal data[501]

(…)[502]

[501] Cion scrutiny reservation against deletion. DE wanted to reinstate Article 38 with a new paragraph (b) with the following wording: " provide the exchange of insights in the level of protection in third countries; this in particular includes the Member States being notified by the Commission of the progress on and the outcome of assessments in accordance with Article 41 of Regulation (EU) ..../2012 and Article 34(2) and (3) of this Directive;" DE added "in the development and" after *mutual assistance* in paragraph (c) first line. In paragraph 2, DE added "supervisory authorities" and the Commission in the first line and deleted the end of the sentence after *supervisory authorities,* in the third line.

[502] ES meant that if this article 38 was to be removed it could only be on the basis that within the GDPR the international cooperation is covered with an extensive view and with the scope of this directive included.

CHAPTER VI

INDEPENDENT SUPERVISORY AUTHORITIES [503]

SECTION 1

INDEPENDENT STATUS

Article 39

Supervisory authority

1. Each Member State shall provide that one or more independent public authorities[504] are responsible for monitoring the application of the provisions adopted pursuant to this Directive.

1a. Each supervisory authority shall contribute to the consistent application of this Directive throughout the Union. (…) For this purpose, the supervisory authorities shall co-operate with each other and the Commission.

---

[503] DE, EE, ES and FR scrutiny reservations. ES said that the scrutiny reservation was linked to the need for consistency with the GDPR and meant that it was necessary to wait until a clear conclusion on the GDPR was reached. The Chair indicated that when the Articles equivalent to Articles 39 to 43 in the Directive were discussed in the context of the Regulation; the delegations then found that Article 39 was too prescriptive. EE welcomed the approach to align the two texts. IE, FI and SE meant that Chapter VI should be consistent with corresponding Articles in GDPR unless there are specific reasons related to the scope of the Directive for the adoption of different rules. AT, BE, DE, DK, CH, CZ, FI, HU, IT, PT and SI thought that it would be better to finalise the GDPR before discussing this text. Cion accepted this suggestion on method. CZ supported taking over most solutions developed in relation to the GDPR, with some exceptions due to special nature of the controllers and the public interest underlying the processing (no need for one-stop-shop etc.). SE, while understanding the need for further harmonization, requested that MS be given more room for manoeuvre, the text was still too detailed. SE also requested that it should be possible to have more than one supervisory authority with different tasks and powers.

[504] RO found the expression *independent public authorities* unclear and suggested to provide more details and specifications to eliminate ambiguities.

2. Member States may provide that a supervisory authority established (…) under Regulation (EU)…./2012 assumes responsibility for the tasks of the supervisory authority to be established under paragraph 1 of this Article.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which (…) shall represent those authorities in the European Data Protection Board.

Article 40

Independence

1. Member States shall ensure that each supervisory authority acts with complete[505] independence in performing the **tasks** and exercising the powers entrusted to it [506].

2. (…) Member States shall provide that the member or the members of the supervisory authority, in the performance of their duties [507], remain free from external influence, whether direct or indirect.[508]

3. (…)[509]

4. (…)[510]

---

505 ES said that the word *complete* was not necessary and could be misleading in some cases, and suggested to keep the same solution as in the GDPR.

506 CZ wanted to add "according to this Directive.", to clarify that independence of DPA is focused on its duties and powers provided for under this Directive whereas it has to follow relevant decisions or instructions in other cases.

507 CZ wanted to add "according to this Directive.", to clarify that independence of DPA is focused on its duties and powers provided for under this Directive whereas it has to follow relevant decisions or instructions in other cases.

508 HU meant that arts of Article 47.2 were missing in the Directive and wished to see uniform texts on this . CZ wanted to add "in accordance with this Directive". AT, DE and CH wanted to add " and neither seek nor take instructions from anybody." in the end of the sentence, as is Article 47 of the GDPR.

509 Cion and AT scrutiny reservation against deletion. DE also preferred to reinstate paragraph 3, but using the singular or plural for the members.

510 Cion and AT scrutiny reservation against deletion. DE also preferred to reinstate paragraph 4 but using the singular or plural for the members.

5. (…) Member States shall ensure that each supervisory authority is provided with the (…) human, technical and financial resources, premises and infrastructure necessary for the effective performance of its **tasks** and exercise of its powers including those to be carried out in the context of mutual assistance, co-operation and active participation in the European Data Protection Board.

6 (…) Member States shall ensure that each supervisory authority must have its own staff which shall be appointed by and[511] be subject to the direction of the member or the members of the supervisory authority.

7. Member States shall ensure that each supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that each supervisory authority has separate **public** [512]annual budgets **which may be part of the overall state or national budget and**[513] shall be made public.[514]

Article 41

General conditions for the members of the supervisory authority [515]

1. Member States shall provide that the member or the members of each supervisory authority must be appointed either by the parliament or the government or the head of state of the Member State concerned [516].

[511] IE wanted to delete "be appointed by and" since it meant that the staff of the SA should be appointed by an independent process and not by the member(s) of the SA.

[512] To align with GDPR.

[513] To align with GDPR.

[514] To align with GDPR. CH reservation on paragraph 7 if it was not aligned to Article 47.7 in GDPR.

[515] HU meant that Article 41 in the Directive was not completely aligned tot he text in the GDPR. LV suggested to refer to the GDPR for Articles 41-43 instead of aligning the text.

[516] DE and AT suggested adding " or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure. RO wanted that only the national parliament appoint the SA to ensure a real and institutional independence and also according to the Schengen Convention.

2. The member or members shall have the qualifications, experience and skills required to perform their duties and exercise their powers.

3. (…)[517]

4. (…)[518]

5. (…)[519]

Article 42

Rules on the establishment of the supervisory authority

Each Member State shall provide by law for:

(a) the establishment of each supervisory authority (…);

(b) (…)

(c) the rules and procedures for the appointment of the member or members of each supervisory authority (…);

(d) the duration of the term of the member or members of each supervisory authority, which shall be [520] no less than four years, except for the first appointment after entry into force of this Directive, part of which may take place for a shorter period;

(e) whether and, if so, for how many terms, the member or members of the supervisory authority shall be eligible for reappointment;

[517] Cion scrutiny reservation against deletion.
[518] Cion and AT scrutiny reservation against deletion.
[519] Cion and AT scrutiny reservation against deletion.
[520] DE suggested adding: " more than eight years or no" before *four years.*

(f) the (…) conditions governing the employment of the member or members and staff of each supervisory authority and rules governing the cessation of employment. [521]

(g) (…)

Article 43

Professional secrecy[522]

Member States shall provide that the member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy *both during and after their term of office* [523]with regard to any confidential information which has come to their knowledge in the course of the performance of their duties or exercise of their powers, (…).

[521] DE suggested that paragraph (f) reads as follows " (f) the (…) conditions governing the **duties of the member or members of staff of each supervisory authority, including prohibition on actions and occupations incompatible therewith during and after the term of office and rules governing ~~the~~** employment of the member or members and staff of each supervisory authority and rules governing the cessation of employment.

[522] IE suggested to move the text of Article 43 to Article 40.

[523] IE suggestion. IE meant that the words *both during and after their term of office* should be moved to after *professional secrecy*~~.~~

SECTION 2

TASKS AND POWERS

Article 44

Competence

1. Member States shall provide that each supervisory authority shall be competent to perform the **tasks** and to exercise (…) the powers conferred on it in accordance with this Directive on the territory of its own Member State.

2. Member States shall provide that the supervisory authority is not competent to supervise [524]processing operations of independent judicial bodies[525] when acting in their judicial capacity [526]. [527]

Article 45 [528]

Tasks

1. Member States shall provide that the supervisory authority:

   (l) monitors and enforces the application of the provisions adopted pursuant to this Directive and its implementing measures;

---

524 DE suggested adding "decisions and " before *processing operations.*

525 DE suggested to replace the underlined text with "courts" as was used in the Cion proposal because DE and CH found that the expression independent judicial body was unclear. CH preferred the wording of recital 55, CH suggested to replace *independent judicial bodies* with "national courts or other judicial authorities".

526 ES suggested adding "and other matters assigned to bodies or authorities of the judiciary related to their judicial capacity." ES meant that such wording was necessary to ensure the independence of the judiciary enshrined in the Constitutions of the MS, so that all treatments related to the judicial capacity fell outside the administrative control, and remained within the judiciary.

527 DE and HU scrutiny reservation. DE welcomed the independence of the judiciary. SI considered that the prosecution office and the police should be put on equal footing with the judiciary and be excluded for the SA supervision. Cion scrutiny reservation.

528 For FR it was not possible to just copy the equivalent rules from the GDPR.

(aa) promotes public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data;[529]

(ab) promotes the awareness of controllers [530] and processors of their obligations under the provisions adopted pursuant to this Directive;

(ac) upon request, provides information to any data subject concerning the exercise of his or her rights under the provisions adopted pursuant to this Directive and, if appropriate, co-operates with the supervisory authorities in other Member States to this end;

(m) deals with complaints lodged by any data subject, or by a body, organisation or association representing and duly mandated by that data subject in accordance with Article 50, and investigates, to the extent appropriate, the subject matter of the complaint and informs the data subject or the body, organisation or association of the progress and the outcome of the investigation within a reasonable period[531], in particular where further investigation or coordination with another supervisory authority is necessary [532];

(n) checks the lawfulness of data processing pursuant to Article 14, and informs the data subject within a reasonable period on the outcome of the check or on the reasons why the check has not been carried out; [533]

(o) **cooperates** with**, including sharing information, and** provides mutual assistance to other supervisory authorities with a view to ensuring the consistency of application and enforcement of the provisions adopted pursuant to this Directive;

---

529 DE did not see any meaning in paragraph (aa) so it suggested to delete it.

530 DE suggested to add "their representatives" after *controller*.

531 RO required a clarification of the words *reasonable time* and suggested to set out a maximum deadline.

532 DE suggested to add " whereby Article 11b (1) shall apply mutatis mutandis to the notification by the supervisory authority;"

533 DE suggested to delete paragraph (c) since it does not add anything more than paragraph (b), Article 14 should also be removed.

(p) conducts investigations on the application of the provisions adopted pursuant to this Directive either on its own initiative, **including on the basis of a information received from** another supervisory **or other public authority, or in response to a** a complaint **(…);**

(q) monitors relevant developments insofar as they have an impact on the protection of personal data, in particular new technologies, mechanisms or procedures involving specific risks for the rights and freedoms of individuals;

(r) responds to consultation requests by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;

(s) gives advice on processing operations referred to in Article 26;

(t) contributes to the activities of the European Data Protection Board.

2. (…)

3. (…)

4. (…)

5. Member States shall provide that the performance of the **tasks** of the supervisory authority shall be free of charge for the data subject.

6. Where requests are manifestly unfounded or excessive, in particular due to their repetitive character, the supervisory authority may refuse to act on the request [534]. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

[534] CH suggested to add *can charge a fee* and to delete the last sentence.

Article 46

Powers[535]

Member States shall provide that each supervisory authority shall have at least the following powers [536]:

(a) investigative powers (…);[537]

(b) effective powers of interventions (…);[538]

(c) the power to engage in legal proceedings[539] where the provisions adopted pursuant to this Directive have been infringed or to bring this infringement to the attention of judicial or other relevant authorities. [540]

[535] PT and RO asked about the differences between Articles 45 and 46 and according to what criteria the divisions would be made. DE, EE, CZ thought that the powers were not sufficiently defined. UK supported Article 46 in principle and underlined that there must not be a conflict between the SA and "legitimate reason". Cion stressed that MS had the competence to decide the powers, concerning access, the SA must have access but it was again for the MS to set out the details. SI asked for a binding and closed list and suggested to find the smallest common denominator. Cion scrutiny reservation. CZ would appreciate if the investigative powers and effective powers would be set out in more detail. AT scrutiny reservation.

[536] DE wanted to add "to fulfil its duties" after *powers.*

[537] DE wanted to reinsert the text from the Cion proposal that had been deleted.

[538] DE wanted to reinsert part of the text of Cion proposal as follows: " (b) effective powers of interventions**,** such as the delivering of opinions before processing is carried out and ensuring appropriate publication of such opinions, (…) or warning or admonishing the controller, or referring the matter to national parliaments or other political institutions" and meant that the examples should be understood as alternatives**.**

[539] EE asked what the terms "engage in legal proceedings" meant.

[540] FR did not approve "or". DE wanted it to be set out clearly that the MS had the choice between legal proceedings or to bring infringements to an authority.

Article 47

Activities report

Member States shall provide that each supervisory authority draws up an annual[541] report on its activities [542]. The report shall be made available to the Commission and the European Data Protection Board.

[541] DE wanted to delete *annual.*

[542] DE wanted to add " at least every two years

CHAPTER VII

CO-OPERATION[543]

Article 48

Mutual assistance[544]

1. Member States shall provide that supervisory authorities provide each other with mutual assistance in order to implement and apply the provisions adopted pursuant to this Directive (…) and shall put in place measures for effective co-operation with one another. Mutual assistance

[543] FR reservation on the whole chapter until the text of GDPR is finalised. FI and DE commented that the Articles corresponding to Articles 48- 55 in the Directive were drafted in a much broader way. FI thought generally that article 48 would be clarified by aligning it more closely with article 55 of GDPR. AT also noted that detailed rules on *e.g. in what cases and/or under what conditions mutual assistance may be refused, purpose limitation provision or a rule stipulating who bears the costs* that were set out in the GDPR were missing (Articles 55. 3-4 and 7) FR thought that it would be useful to examine the Chapter on the basis of the following two points: 1) the exercise of the rights of the data subject where he or she belongs to a Member State other than that of the supervisory authority; and 2) the link between the rules that must be respected by the Member States in order to exchange data with third countries and the rules that must be observed by the European Union agencies on this question (two instruments under revision concerning Europol and Eurojust). IE meant that the Chapter should be consistent with the corresponding provisions in the GDPR, subject to the need to take account of the specific requirements of the police and judicial authorities in the area of criminal justice. IE also meant that it was necessary to take into account that this instrument was a Directive and thus does not require the same level of detail as the GDPR. ES found that a greater consistency with the GDPR should be pursued.

[544] SI reservation. DE and FR scrutiny reservation. FR was in favour of the principle in the Article but asked about the scope and the type of obligations to be put in place. ES was also in favour and thought that it would allow a certain level of harmonization and reduce the current asymmetries that enable certain actors to decline or delay collaboration.
EE said that MS would not want to share data relating to national security. At CH request for clarity on Schengen aspects the Chair informed that Schengen aspects would be dealt with later. SE questioned that a SA from one MS could oblige a SA in another MS to carry out inspections and investigations. SE meant that if such possibilities should be accepted both substantial and formal refusal grounds must exist. IE wanted the following elements to be addressed in the Article: a) the requesting supervisory authority to provide all necessary information, including the purpose of the request and the reasons for the request; b) limit the use of information provided under this article to the purpose for which it was requested; c) enable a supervisory authority to refuse a request for mutual assistance in specified circumstances, in particular where compliance with the request would be incompatible with Union or Member State law to which the supervisory authority receiving the request is subject.

shall cover, in particular, information requests and supervisory measures, such as requests to carry out (…) inspections and investigations. [545]

2. Member States shall provide that a supervisory authority takes all appropriate measures required to reply to the request of another supervisory authority. [546]

3. The requested supervisory authority shall [547]inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority. [548]

[549]

[550]

[551]

---

[545] DE thought that Article 48.1 could create problems since the instrument is a Directive. Cion scrutiny reservation. FR wanted clarification as regards the links between paragraph 1 and 2 and 3, *e.g.* does paragraph 1 determine the scope of paragraphs 2 and 3.

[546] AT suggested to add "without undue delay" at the end of paragraph 2 and FI to copy Article 55.2 in GDPR.

[547] AT wanted to add " without undue delay and no later than within one month after having received the request," before *inform.*

[548] FI and DE wanted to align Article 48.3 to Article 55.5 in GDPR and adding the following text: "The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested." (art. 55.3 in GDPR). FR asked to see examples of consequences of failure to comply with paragraphs 2 and 3.

[549] FI and CZ suggested adding a new paragraph 4 stipulating when it is possible to refuse to comply to the request (art. 55.4 in GDPR).

[553] FI and DE wanted to add a new paragraph: **"**5. Member States shall provide that supervisory authorities supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format.**"** (art. 55.6 in the GDPR). CH suggested adding a paragraph 4 with the following wording: **. "**A supervisory authority to which a request for assistance is addressed may refuse to comply with it when:
(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or(b) compliance with the request would be incompatible with the provisions of this Directive or with Union or Member State law to which the supervisory authority receiving the request is subject."

[551] CZ, FI and DE suggested adding a new para 48.7 as follows: "Member States shall provide that no fee is charged for any action taken following a request for mutual assistance." (art. 55.7 in GDPR).

552

Article 49

Tasks of the European Data Protection Board [553]

1. The European Data Protection Board established by Regulation (EU)…./2012 shall exercise the following tasks in relation to processing within the scope of this Directive:

(a) advise the Commission on any issue related to the protection **[554]**of personal data in the Union, including on any proposed amendment of this Directive;

(b) examine, on request of the Commission or on its own initiative or of one of its members, any question covering the application of the provisions adopted pursuant to this Directive and issue guidelines**[555]** recommendations and best practices (…) in order to encourage consistent application of those provisions; **[556]**

(c) review the practical application of guidelines**[557]**, recommendations and best practices referred to in point (b) (…);

---

552 FI adding a new para 48.8 about the Commission´s role in specifying the format and procedures for the exchange of information similar to art. 55.10 in GDPR.

553 SI reservation. DE and FR scrutiny reservations. FR wanted to wait until the text of the Articles to which reference is made is consolidated. While supporting the Article the UK asked to clarify the relationship between European Data Protection Board and the Cion. FI wanted to add the text in Article 66.1(g) to the draft Directive. BE asked the addition of a recital to clarify that the DPA designated by the MS to be a member of the Board in the context of this Directive could be another than the one designated for the GDPR.

554 CZ suggested to add "and free movement" after *protection* to be in line with Article 1.2.

555 CZ suggested to delete *guidelines* since it might be understood as interfering with the independence of the DPAs.

556 Paragraph 1 letters (b) and (c) were problematic according to DE.

557 CZ suggested to delete *guidelines* since it might be understood as interfering with the independence of the DPAs.

(d) give the Commission [558]an opinion on the level of protection in third countries or international organisations;[559]

(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;

(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;

(g) promote the exchange of knowledge and documentation [560]with data protection supervisory authorities worldwide, including data protection legislation and practice.

2. Where the Commission requests advice from the European Data Protection Board, it may lay out [561]a time limit[562] within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.

3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission [563]and to the committee referred to in Article 57(1) and make them public.

---

[558] BE and DE asked to insert "and the Member States".

[559] FI wanted to add the following text in the end of the paragraph: in particular in the cases referred to in article 34. DE said that the MS should also be allowed to receive this information. In order to make it clear that the European Data Protection Board is entitled to give an opinion when the Commission adopts adequacy decisions pursuant to Article 34, AT suggested to add the following: "especially with regard to the adoption of an adequacy decision pursuant to Article 34" after *international organisation.*

[560] FI wanted to delete the text after *documentation* and replace it with the following text: "on data protection legislation and practice with data protection supervisory authorities worldwide"

[561] CZ and FI suggested to replace *lay out* with *indicate* so as to align the text with Article 66.2 of the GDPR and stress the independence of the EDPB.

[562] FI wanted to use the same vocabulary *indicate a time limit* as in Article 66.2 of the Regulation.

[563] BE asked to add "and the Member States" since such texts would help the correct application of the proposed Directive.

4. The Commission shall inform the European Data Protection Board[564] of the action it has taken following opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.

[564] DE meant that the MS should be informed about this as well and wanted a parallelism between GDPR and the Directive on this.

CHAPTER VIII

REMEDIES, LIABILITY AND SANCTIONS [565]

Article 50

Right to lodge a complaint with a supervisory authority[566]

1. Without prejudice to any other administrative or judicial remedy, Member States shall provide that each supervisory authority shall deal with complaints lodged by any data subject [567](…) if he or she considers that the processing of personal data relating to him or her [568]does not comply with provisions adopted pursuant to this Directive. [569]

---

565 IE meant that the Chapter should be consistent with the corresponding provisions in the GDPR, subject to the need to take account of the specific requirements of the police and judicial authorities in the area of criminal justice. IE also meant that it was necessary to take into account that this instrument was a Directive and thus does not require the same level of detail as the GDPR. DE meant that the provisions of this Chapter and Chapter VIII of GDPR should correspond in principle, taking into account special features for the police and justice area, and that it theremore made sense to wait for the discusssion on the GDPR to be completed.

566 SI objected Article 50 since it would lead to forum shopping. EE said that this provision was against their law. Cion stated that a SA would not be operating in another MS but would only be operating in its MS so there would be no forum-shopping. Cion scrutiny reservation. SE meant that it should be made clear that this Article did not imply an obligation for the SA to receive complaints that it is not competent to deal with, cfr Article 44. FI considered that the data subject should have the right to lodge a complaint to any supervisory authority within EU, but that only the competent SA should be allowed to deal with complaints lodged by data subjects and if a complaint has been lodged to another than the competent SA that SA should *ex officio* transmit the complaint to the competent SA. FI wanted to decide the exact wording of Article 50 once the text in GDPR had been decided.

567 FR did not think that data subjects should be able to lodge their complaints with any Union authority, and considered that these possibilities of redress should be limited to the supervisory authorities of the controller's MS only. IE meant that the paragraph needed to be amended to specify that a SA authority is competent only for complaints concerning competent authorities in the SA's own MS. IE found that that the SA role should be confined to directing the data subject to the competent SA or passing on the complaint and informing the data subject accordingly.FR said that in the GDPR a consensus was agreed that a derogation from the one-stop shop mechanism be laid down for public authorities, in the Directive, which is geared mainly to public authorities, such a derogation should be the rule. AT meant that the current wording was unacceptable because it encouraged forum shopping but could support the wording if the SA that had received a complaint was not obliged to forward the complaint to the competent SA.

568 CZ wanted to add *for which the Supervisory Authority is competent* after *her*. CZ meant that it was desirable that the data subject should be able to lodge a complaint to any SA, *e.g.* of his/her residence, then it should be set out that each SA shall forward a complaint for which it was not competent to the relevant SA of the relevant MS.

569 The Chair stated that Article 50.1 provided for the possibility to lodge a complaint in any MS. AT, supported by SE, considered it important to clarify so as to avoid forum shopping. In the same vein DE asked to clarify which SA was competent. Support from CH, CZ, EE. DE suggested the

2. For the situation referred to in paragraph 1, Member States may provide for the right of any body, organisation or association which (…) has been properly constituted according to the law of a Member State to lodge the complaint [570]with a supervisory authority on behalf of the data subject (…).[571]

3. (…)

Article 51

Right to a judicial remedy against a supervisory authority[572]

1. Without prejudice to any other administrative or non-judicial remedy, Member States shall provide for the right to a judicial remedy against decisions of a supervisory authority.

---

following text for paragraph 1: "Without prejudice to any other administrative or judicial remedy, Member States shall provide that each **of its** supervisory authorit**ies**~~y~~ shall deal with complaints lodged by any data subject (…) if he or she considers that the processing of personal data relating to him or her does not comply with **the Member States'** provisions adopted pursuant to this Directive. **If the supervisory authority is not competent for the controller or processor mentioned in the complaint, Member States shall provide that the supervisory authority shall hand the complaint over to the competent supervisory authority."** DE thereby wanted to make clear that only the supervisory authority competent under national law for the controller or processor mentioned in the complaint is to review the matter and take any necessary action. To solve the issue of effective judicial review requiring that any non-competent supervisory authority called on must forward the complaint to the competent supervisory authority could be one way forward.

570 DE suggested the following text for the end of the sentence, after *complaint:* "**if it is representing and duly mandated by**[570] ~~on behalf of~~ the data subject (…)."

571 BE asked that paragraph 2 was deleted. FR reservation. FR indicated that it had entered a reservation on the introduction of this type of remedy in the GDPR. IE and AT supported the discretion given to MS in paragraph 2. ES wanted to reduce the scope of paragraph 2, in the Article as well as in a recital, by establishing that the body, organisation or association must be duly and expressly mandated to be allowed to act on behalf of the individual affected by the processing operation.

572 FI asked whether a SA would be obliged to forward a complaint to the competent SA. DE scrutiny reservation.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a judicial remedy where the supervisory authority does not deal with the complaint [573](…) or does not inform the data subject[574] within three months[575] on the progress or outcome of the complaint lodged under Article 50. [576]

3. (…)[577]

Article 52

Right to a judicial remedy against a controller or processor[578]

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority under Article 50, Member States shall provide for the right of data subjects to a judicial remedy if they consider that their rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of their personal data in non-compliance with these provisions.

Article 53

Common rules for court proceedings [579]

(…)

[573] SE meant that according to the subsidiarity principle it was not possible to introduce a right to judicial remedy when a SA has failed to act, since this would mean an harmonisation of MS procedural rights, paragraph 2 should therefore be deleted or redrafted.

[574] RO suggested to add " or by case, the body, organisation or association from Article 50.2" after *data subject* .

[575] FR suggested to extend the deadline. CH suggested to refer to a *reasonable deadline.*

[576] EE opposed paragraphs 2 and 3. BE suggested to delete paragraph 2 since it was a duplication.

[577] Cion scrutiny reservation against deletion.

[578] DE scrutiny reservation.

[579] Cion scrutiny reservation against deletion. FR and FI welcomed the deletion. While considering the application of the Directive on judges as a horizontal issue, IE thought that Articles 52 and 54 should not apply to judges when exercising judicial functions.

Article 54

Liability and the right to compensation[580]

1. Member States shall provide [581]that any person who has suffered damage[582] as a result of (…) a processing operation which is non compliant with the provisions adopted pursuant to this Directive shall have the right to receive compensation from the controller or the processor[583] for the damage suffered. [584]

2. Without prejudice to Article 20, where more than[585] one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage. [586]

---

580 UK pointed at the fact that the processor was not responsible and considered that this must be solved in both the Directive and the Regulation. While considering the application of the Directive on judges as a horizontal issue, IE thought that Articles 52 and 54 should not apply to judges when exercising judicial functions. FI meant that an individual employee of a public authority (e.g. the police forces), agency or any other body should be excluded from the liability of damages which occur in the course of the regular activities of that body. AT thought that substantive arrangements regarding compensation should not be regulated in detail in the Directive but left to the MS, like in Article 19 of DPFD. AT wanted it to be clarified that the liability was fault-based and not a strict liability, either in the Article or in a recital.

581 CZ suggested to insert the following text after *provide* "in compliance with its general rules on liability for damages" since this Directive cannot change national law of liability.

582 SE and DE wished it to be clarified that the damage could be both economic and non-pecuniary losses; DE said that if it covered also non-pecuniary damage liability for such losses could not be unlimited. DE meant that if Article 54 also included non-material damage, the MS should at least have the discretion to specify the liability.

583 FR and DE found it inadvisable to include the processor in the joint liability of controllers and FR suggested to delete the reference to *processor* in this Article. DE found it necessary to determine whether mandatory liability of the processor is necessary but said that the MS were supposed to be given some discretion here.

584 BE asked for the addition of a recital indicating that the data subject has to proof the damage, the fact causing the damage and the link between the damage and the fact.

585 BE suggested to replace "more than" with "at least" to cover situations when there is one controller and several processors. BE wanted the addition of a recital with the following wording "jointly and severally liable" setting out that each liable controller or processor has to pay for all the damage.

586 CZ suggested to delete paragraph 2. SE and IE wanted to analyse the consequences of the joint responsibility and SE also of the rule on the onus of proofs. SE suggested to clarify that the joint responsibility was limited to cases when more than one controller has *caused* the damage. RO wanted to add "according to the national law" at the end of the paragraph. AT meant that paragraph 2 only set out for joint and several liability within a group of several data controllers and/or several processors, not joint and several liability between one data controller and one processor.

3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or processor proves that they are not responsible for the event giving rise to the damage. [587]

Article 55

Penalties[588]

Member States shall lay down the rules on penalties, applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive.

[589]

[587] BE, supported by CZ and PL, suggested to delete paragraph 3.

[588] DE, ES, RO scrutiny reservation on Article 54, RO in relation to *national law*. CH, EE opposed this Article because ~~EE~~ their respective national law did not allow for penalties on public bodies. CH, and EE reservation. Cion stated that Article 55 existed in the Regulation as well and was a standard provision. CZ considered that the Article required a substantial revision, notably as regards sanctions on public authorities, certain provisions are so imprecise that general sanctions for non-compliance would be contrary to the rule of law and the corresponding Article 79b in GDPR is completely uncertain. AT wanted to keep the Article so that the level of protection did not go below the level of DPFD.

[589] ES wanted to clarify that financial corrective measures against the public sector cannot be adopted and therefore suggested to insert a new paragraph with the following wording: "Only non-financial corrective actions may be adopted on public authorities and bodies established in a Member State. Each Member State may lay down the rules on whether these actions may be adopted."

CHAPTER IX

(…) IMPLEMENTING ACTS

Article 56
Exercise of the delegation

(…)[590]

Article 57

Committee procedure[591]

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. [592]

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.[593]

---

590 Cion scrutiny reservation against deletion.

591 FR reservation. FR noted that the discussion on the committee procedure and delegated acts was suspended in the context of the GDPR until the end of the discussions on the text.

592 DE wanted to add a sentence setting out that the Cion could not adopt implementing acts without the Committee's opinion: "The Commission shall not adopt the draft implementing act where no opinion of the committee is delivered."

593 DE suggested to delete paragraph 3 to take account of the suggested removal of Article 34.5.

CHAPTER X

FINAL PROVISIONS

Article 58

Repeals

1. Council Framework Decision 2008/977/JHA is repealed.

2. References to the repealed Framework Decision referred to in paragraph 1 shall be construed as references to this Directive.

Article 59

Relationship with previously adopted acts of the Union for judicial co-operation in criminal matters and police co-operation

The specific provisions[594] for the protection of personal data with regard to the processing of personal data by competent public authorities for the purposes (…) referred to in Article 1(1) in acts of the Union[595] adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive remain unaffected. [596]

[594] SE asked for a clarification on what was meant with *special provisions.*

[595] PL, IT, SE and UK asked which acts were referred to here.

[596] DE scrutiny reservation.

Article 60

Relationship with previously concluded international agreements in the field of judicial co-operation in criminal matters and police co-operation[597]

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to the entry force of this Directive and which are in compliance with Union law applicable prior to the entry into force of this Directive shall remain [598]in force until amended, replaced or revoked. In accordance with the Treaties, to the extent that such agreements concluded by Member States are not compatible with Union law, the Member State or States concerned shall[599] take all appropriate steps to eliminate the incompatibilities established. [600]

---

597 CH and DE scrutiny reservations. For the UK and CZ Article 60 as it was drafted here was unacceptable. SI said that DPFD was more acceptable and that the text contained no element of flexibility. FR requested the insertion of a grandfather clause, in order to preserve the MS operational exchange channels. FR recalled the link between Article 60 and Chapter V. FR pointed in particular to the fact that the simultaneous promotion of strict rules in Chapter V and the obligation to denounce agreements pursuant to Article 60 would lead to the prohibition of data exchanges which are essential for legitimate public interest aims.
CZ and FR noted that there were no time limits/transition periods foreseen, which entails a more immediate obligation for the MS to denounce and renegotiate their "non-compliant" agreements. FI found the text very ambiguous. For AT the core problem was the dependence on the relevant third countries and that it remained unresolved despite that the-year period for the renegotiation of agreements no longer applied. AT meant that the aim should still be to adapt as soon as possible agreements that do not conform to the provisions of the Directive. AT suggested that intermediate solutions be set out in a recital.

598 BE, supported by CZ, suggested to add "unaffected." and delete the rest of the text of the paragraph so that Article 60 is in line with Article 59 in fine. FR could alternatively agree the Article in line with the BE/CZ suggestion to delete the last sentence. ES could accept the current wording but preferred the deletion of the second sentence. PL supported the deletion of the second sentence of the Article. BE asked it to be clarified what would happen if the Cion withdraw an adequacy decision, would the MS need to renegotiate the agreement. CZ said that first sentence provided for *lex specialis* as regards these agreements, the second sentence was therefore not necessary, it was even contradictory. CZ said that such agreements may well be amended and then the amended wording will remain in force; it could even be said that this is the usual result of amending something, at least in the area of international law.

599 CH suggested inserting "as far as possible".

600 AT considered the Article inflexible. CY scrutiny reservation. BE, CH, IT and CZ objected Article 60. CH asked what would happen when there it was need to revoke the agreement but that another Party to the agreement would refuse to renegotiate it. Cion reservation. DE suggested to reword Article 60 as follows: "International agreements involving the transfer of personal data **processed by competent authorities for the purposes referred to in Article 1(1)**[600] to third countries or international organisations which were concluded by Member States prior to the entry into force of this Directive and which are in compliance with Union law applicable prior to the entry into force of this Directive shall remain **unaffected**in force until amended, replaced or revoked. **To** In accordance with the Treaties, to the extent that such agreements concluded by Member States are not compatible with **this Directive**Union law, the Member State or States concerned shall take **make** all appropriate **efforts** ~~steps~~ to eliminate the incompatibilities established." DE aligned the first sentence to Article 59 and clarified that existing agreements did not need to be renegotiated.

Article 61

Evaluation

1. The Commission shall evaluate the application of this Directive.

2. The Commission shall review within five[601] years after the entry into force of this Directive other acts adopted by the European Union which regulate the processing of personal data by competent public authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, in particular those acts adopted by the Union referred to in Article 59, in order to assess the need to align them with this Directive and make, where appropriate, the necessary proposals to amend these acts to ensure a consistent approach on the protection of personal data within the scope of this Directive. [602]

[601] DE meant that this revision should take place earlier so as to align other acts to the Directive.

[602] DE wanted to add a sentence in the end of paragraph 2 to clarify that the same minimum standards must apply to the EU bodies as to the Member States: "The Commissions proposals shall ensure that the data protection provisions applicable to institutions, bodies, offices and agencies of the European Union within the scope of Article 1(1) at least correspond to the standard set by this Directive."

3. The Commission shall submit reports on the evaluation and review of this Directive pursuant to paragraph 1 to the European Parliament and the Council at regular intervals. The first reports shall be submitted no later than four years after the entry into force of this Directive. Subsequent reports shall be submitted every four years thereafter. The Commission shall submit, if necessary, appropriate proposals with a view of amending this Directive and aligning other legal instruments. The report shall be made public.

Article 62

Implementation

1. Member States shall adopt and publish, by [date/ two years[603] after entry into force] at the latest, the laws, regulations and administrative provisions[604] necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions.

   They shall apply those provisions from xx.xx.201x [date/ two[605] years after entry into force].

   When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.[606]

---

603 For DE, ES, FI and SE two years was too short. CZ, DE and RO preferred three or four years, BE five years and FR three years.

604 BE asked an explanation of what was meant with *regulations and administrative provisions.*

605 DE wanted that the provisions be applicable four years after the entry into force.

606 BE and AT asked how the last sentence of the first paragraph of Article 62.1 and Article 62.2 were linked and AT asked for the removal of paragraph 2.

Article 63

Entry into force and application

This Directive shall enter into force on the first day following that of its publication in the *Official Journal of the European Union*.

Article 64

Addressees

This Directive is addressed to the Member States.
